Pour une justification des articles 25 et 26 de la directive européenne 95/46 CE en matière de flux transfrontières et de protection des données

Poullet, Yves

Published in:
Ceci n'est pas un juriste.. mais un ami. Liber Amicorum Bart De Schutter

Publication date:
2003

Document Version
le PDF de l'éditeur

Yves Poullet

Pour une justification des articles 25 et 26 de la directive européenne 95/46 CE en matière de flux transfrontières et de protection des données

Cet article est la version corrigée et amplifiée du texte présenté à la conférence organisée par l'Union européenne « on the Implementation of the Data Protection Directive » (Bruxelles, 30 septembre - 1 octobre 2002)[1]

> "The worth of a State, in the long run, is the worth of the individuals composing it... a state which dwarfs its men, in order that they may be more docile instruments in its hands even for beneficial purposes, will find with small men no great thing can really be accomplished and that the perfection of machinery to which it has sacrified everything, will in the end avail nothing, for want of the vital power which, in order that the machine might work more smoothly, it has preferred to banish."
>
> John Stuart Mill, On Liberty

Propos liminaires

1. L'idée de dédicacer cet article à l'ami Bart s'explique par deux raisons. La première est notre combat commun au sein de la Commission belge de protection de la vie privée. Tant de rapports communs, tant de points de vue également partagés me donnent l'audace de croire que même sur un thème que nos discussions en matière de protection des données ne nous

L'auteur remercie chaleureusement Melle Veronica Perez du Crid pour son importante contribution à l'article , Mme Marie-Hélène Boulanger et Mr Ulf Brühan pour leurs relectures et suggestions.

ont pas permis d'aborder, nos points de vue doivent être communs. Cet article est donc une invitation à la réponse. Son propos tend à justifier l'attitude internationale de l'Union européenne en matière de flux transfrontières et de protection des données à caractère personnel. En particulier, il légitime l'action de l'Union européenne et des Etats membres en faveur de la protection des données initiée notamment mais non uniquement sur base des articles 25 et 26 de la directive européenne 95/46 dont le contenu fait l'objet d'un bref rappel. Pourquoi ce thème? seconde raison de cet hommage personnel à Bart... Bart, de pars sa stature – et je n'évoque pas ici celle physique qui est à la dimension de celle scientifique et de son engagement – ne s'est jamais senti autant à l'aise que dans les enceintes internationales où il aime cette confrontation des cultures et se distingue par l'écoute respectueuse de celles-ci. Notre propos part de cette même préoccupation: il s'agit modestement d'écouter le point de vue de l'autre, en particulier celui proposé par les Etats-Unis et de mesurer à l'aune de ce point de vue l'importance donnée par l'Europe à ce souci de la protection des données.

Mais revenons au sujet. Le raisonnement s'opère en deux temps:

- le premier (Titre I) démontre de manière négative que les actions européennes prévues par les trois articles ne sont en aucune manière contraires aux traités signés dans le cadre de l'Organisation Mondiale du Commerce (OMC);
- le second (Titre II) affirme le devoir de l'Union européenne et par là des Etats membres de garantir sur le plan international la protection des données collectées à partir de l'Union européenne et décrit les implications tant internes qu'externes de ce devoir.

2. La portée des articles 25 et 26 de la directive 95/46 de l'Union européenne peut aisément se résumer comme suit: la dimension internationale des flux d'informations y compris nominatives rendrait vaine l'existence d'une réglementation dont l'effectivité couvrirait le seul territoire européen. Les autoroutes de l'information que préfigure la toile d'Internet favoriseront encore cette circulation sans frontières, qu'il s'agisse de flux liés à la mobilité des personnes, de flux liés à un commerce électronique croissant ou à la consultation de sites étrangers, de flux liés à des transmissions dans un groupe d'entreprises, à l'intérieur d'un secteur, soit enfin de flux intersectoriels.

Cette réalité risque de mettre à mal la protection des données garantie par la directive européenne. Cette dernière entend dès lors réglementer les

flux transfrontières: elle le fait naturellement en assortissant de conditions les flux de données hors Europe, en exigeant que le pays destinataire offre une protection dite adéquate (article 25). Pour certains types de flux, elle acceptera néanmoins des dérogations (article 26.1) voire à défaut, des solutions contractuelles offrant des garanties « équivalentes » (article 26.2). Ces dispositions font l'objet des développements suivants[2].

A. Le principe général: Le texte des alinéas 1 et 2 de l'article 25 – Des caractéristiques de l'approche à la notion de similarité fonctionnelle

3. En vertu de l'article 25.1. de la directive, *« Les Etats membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question offre un niveau de protection adéquat »*. Le principe est donc l'interdiction du transfert, sauf à démontrer le caractère adéquat de la protection offerte dans le pays tiers.

La directive précise ensuite en son article 25.2 que l'appréciation du caractère adéquat de la protection du pays tiers doit tenir compte de « toutes les circonstances relatives à un transfert ou à une catégorie de transferts » et, en particulier, de différents facteurs dont certains sont fonction du transfert considéré, tels la nature des données, la finalité et la durée des traitements, les pays d'origine et de destination et d'autres concernent le niveau de protection offert dans le pays tiers, comme « les règles de droit générales ou sectorielles en vigueur ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées ».

On note que l'article 25 vise toute forme de transfert et n'exige donc pas que le transfert s'appuie sur un traitement préexistant sur le sol européen . Ceci a pour conséquence que le simple envoi de données par la personne concernée elle-même (par exemple lors de la visite d'un site web

2. Cette description résume la présentation de l'auteur à la XIXème Conférence internationale des commissaires à la protection des données (Bruxelles 1998): « Quelques réflexions à propos de l'article 25 de la directive européenne de protection des données » disponible sur le site de la Commission belge de protection des données (http: //www. privacy. fgov.be/ sur l'analyse de ces articles, cf. également B. Havelange et A.-C. Lacoste, Les flux transfrontières de données à caractère personnel en droit européen, *JTDE*, 2001, p. 240 et ss.

situé hors Europe) tombe sous le coup des articles 25 et 26 même si ce transfert n'ait point comme tel l'objet d'un traitement par un responsable sur le sol européen mais est, conformément au texte même de l'article 25, « destiné à faire l'objet d'un traitement après leur transfert ». On peut même considérer que le transfert même non initié par la personne concernée mais directement sollicité par le responsable situé hors Europe du fait de l'implantation par celui-ci de *cookies*, d'*applets Java* sur le disque dur de l'utilisateur, de bavardages du navigateur ou de l'installation de *spywares* tombent sous le coup de l'article 25 et exigent le respect des exigences de ces deux articles de la directive[3].

4. Au-delà de ces réflexions, la notion de « protection adéquate » conduit à une approche qui, à la lecture du texte de l'article 25, se caractérise comme suit:

- une approche au cas par cas: c'est-à-dire que la situation de la protection des données dans un pays tiers est évaluée « par rapport à un transfert déterminé ou une catégorie de transferts ». L'article 25 al. 1 et al. 2 consacre, nous l'avons dit, une approche au cas par cas, flux par flux ou catégorie de flux par catégorie de flux. Une telle analyse est évidemment lourde pour les Etats membres et les articles 25.4 et 25.6 mentionnent deux possibilités pour la Commission de leur simplifier le travail. Il s'agit de constater « conformément » à la procédure prévue à l'article 31 § 2 « qu'un pays tiers assure ou n'assure pas un niveau de protection adéquat ». En d'autres termes, ces paragraphes permettent la constitution par la Commission européenne de « white » ou de « black lists » et à cette dernière d'imposer sa décision valable pour des catégories de transferts, pour un secteur voire pour l'ensemble des flux vers un pays tiers à l'ensemble des pays européens[4];
- une approche souple et ouverte: selon le libellé même de l'article 25.2 l'évaluation doit pouvoir tenir compte à la fois des particularités propres et évolutives des divers flux transfrontières mais également des solutions diverses et évolutives que chaque Etat, voire chaque responsable des données, peut apporter, l'article 25§2 étant purement indicatif à ce propos. L'instrument méthodologique doit refléter cette ouverture et cette souplesse, et être adaptable aux multiples cas rencontrés ou à rencontrer;
- une approche fonctionnelle: c'est-à-dire que la protection s'évalue tant par rapport aux risques d'atteinte à la protection des données, risques générés par le flux en question, que par rapport aux mesures spécifiques ou générales mises en place par le responsable des données dans le pays tiers pour pallier ces risques.

3. Sur ces différents traitements dits « invisibles », le lecteur consultera: J.M. Dinant, Les traitements invisibles sur Internet, document disponible sur le site du Crid http://www.droit.fundp.ac.be/Textes/privacy_law_tech_convergence.rtf.; S. Desrochers, Internet: une maison de verre, disponible sur le site montréalais de Lexum à l'adresse suivante: http://www.lexum.umontreal.ca/internet 99/p6c1.html.

4. A noter les décisions prises par la Commission à propos de différents systèmes jugés adéquats:
Commission Decision 2000/519/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary - O.J. L 215/4 of 25.8.2000;
Commission Decision 2000/518/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland - Official Journal L 215/1 of 25.8.2000
Commission Decision 2000/520/EC of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related frequently asked questions issued by the US Department of Commerce - Official Journal L 215/7 of 25.8.2000
Commission Decision 2002/2/EC of 20.12.2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act - O.J. L 2/13 of 4.1.2002
Cf. également à propos de la protection proposée par la loi récente d'Argentine, l'opinion du groupe dit de l'article 29 émis le 3 octobre 2002 (W.P. 63) disponible sur le site de la Commission européenne à l'adresse suivante:
www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/
On notera que les décisions peuvent être prises sous réserve d'inventaire ou plutôt d'évaluation après quelques années de fonctionnement, ainsi le récent (2 juillet 2002) Working Document on the functioning of the Safe Harbor Agreement émis par le Groupe dit de l'article 29 est particulièrement critique par rapport à l'effectivité de la protection mise en place par le système américain. Le rapport est disponible sur le site du groupe dit de l'article 29 à l'adresse suivante: www.europa.int/comm/internal_market/en/dataprot/wpdocs. A propos de cette évaluation très critique, lire J. Reidenberg, European Commission avoids Privacy disputes with the U.S.A., Privacy Laws and Bus. Int. Newsletter, Feb. 2002, p. 9 et ss.

5. L'évaluation de ces mesures doit se faire sans a priori; il ne peut être question d'imposer les mécanismes européens mis en place selon la directive (pas d' « impérialisme » européen) mais bien d'apprécier dans quelle mesure les objectifs de protection poursuivis par la directive sont rencontrés, de façon originale ou non par un pays tiers[5]. En ce sens, la notion de protection adéquate ne représente en aucune manière un affaiblissement de la protection des données des personnes protégées au départ de la directive. Au contraire, elle crée pour l'évaluateur la nécessité, tout en ne perdant pas de vue les exigences qui fondent selon la directive le besoin de protection, de prendre en considération les adaptations originales des modalités de cette protection, adaptations proposées par les pays tiers. L'instrument méthodologique doit laisser la place à cette variabilité de nature et de portée des solutions apportées, à cette recherche de « similarité fonctionnelle ».

La « similarité fonctionnelle » implique que l'on recherche non la transposition pure et simple des principes et systèmes de protection européens dans le pays tiers, mais bien la présence de tout élément remplissant les fonctions recherchées, même si lesdits éléments doivent être d'une nature différente de ceux que l'on connaît en Europe. Elle permet sans doute un meilleur respect des structures et des caractéristiques juridiques locales qu'un requis de protection équivalente, qui exige une similarité complète, législative en tout cas.

6. Quelques remarques liminaires s'imposent d'emblée au sujet de la notion « d'adéquation », que d'aucuns ont opposé à celle « d'équivalence »[6].

Tout d'abord, cette notion suppose sans doute un référent (qui permette de répondre à la question: « par rapport à quoi la protection doit-elle être adéquate »?). Or, ce référent n'est pas défini, comme tel par la directive. Il n'existe pas de système de référence déterminé par rapport auquel on puisse évaluer la protection du pays tiers. Ensuite, on note que, si les critères énoncés par l'article 25.2 constituent de précieuses indications

Le plus bel exemple est certes la décision de la Commission reconnaissant le caractère adéquat des « Safe Harbor Principles », émis par le département du commerce américain, décision prise le 26 juillet 2000. Pour un commentaire de ces « Safe Harbor » , lire Y. Poullet, « Les Safe Harbor: Une protection adéquate? », IFCLA, Paris 15-16 juin 2000, publié notamment sur le site du Crid: http://www.droit.fundp.ac.be/crid/.

Cf. notamment P.M. Schwartz, European Data Protection Law and Restriction on International Data Flows , 80 Iowa Law Rev., 1995, n°3, pp. 473 et s.

quant aux éléments à prendre en compte pour évaluer l'adéquation de la protection du pays tiers, ils ne constituent pas une liste exhaustive (l'article 25.2 énonce qu'il faut « en particulier » prendre en considération tel ou tel élément). On peut prendre en compte bien d'autres facteurs pour affiner cette analyse, que ces facteurs soient relatifs au flux considéré ou à la protection existant dans le pays tiers.

De nombreuses réflexions[7] ont été émises par le Groupe dit de l'article 29 à propos de la notion de protection adéquate. Elles ont abouti à l'adoption des principes suivants: l'évaluation du critère de la protection adéquate[8] commence par une analyse des risques encourus par les personnes concernées du fait de la transmission des données vers les pays tiers et déduit de cette analyse[9] des critères de « conformité » et d' « effectivité » du système dont le caractère adéquat doit être évalué non en principe mais au regard des risques particuliers révélés par les circonstances de transfert[10].

7. Ainsi, on cite:
   - Article 29 Data Protection Working Party "Discussion Document: First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy", 26 June 1997, WP 4.
   - Article 29 Data Protection Working Party *"Working Document: Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?"*, 14 January 1998, WP 7.
   - Article 29 Data Protection Working Party *"Working Document: Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries"*, 22 April 1998, WP 9.
   - Article 29 Data Protection Working Party *"Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive"*, 24 July 1998, WP 12.

8. «First Guidelines concerning transfers of Personal Data to third countries. Possible means of evaluating the adequate nature of Protection », Discussion Paper adopté par le Groupe dit de l'article 29 le 26 juin 1997, DG XV D/5020/97-Fr-final.

9. A ce propos, outre le document cité à la note précédente et l'Opinion 7/99 du 3 décembre 1999 (WP 27) émise par le groupe de travail de l'article 29 à propos des US « Safe Harbor Principles », on lira l'étude élaborée pour la DG XV par Y. Poullet et B. Havelange, Elaboration of a Methodology to evaluate the Adequacy of the Level of the Protection of the Individuals vis-à-vis the Processing of personal Data in Third Countries (European Commission, Official Publications, Office, ISBN 92-828-4304, 1998), qui a servi de base à l'élaboration des critères repris par le Groupe de Travail dit de l'article 29.

10. « Le risque est un événement dommageable dont la survenance n'est pas certaine mais entraîne pour la personne fichée, un dommage. Dans le cadre de transferts de données personnelles, nous avons classifié les risques en quatre grandes catégories ...: les risques de perte de contrôle, de réutilisation de données, de manque de proportionnalité et d'inexactitude de ces données », Y. Poullet et B. Havelange, op. cit., note 9.

Ces critères ont été systématiquement appliqués dans les analyses auxquelles la Commission s'est livrée dans les cas où elle a dû juger du caractère adéquat des systèmes qui lui étaient soumis.

Le critère de la « conformité » s'adresse au contenu de la protection accordée aux personnes concernées (principe de l'accès, des données sensibles, de la détermination des finalités, etc.). Il reprend une liste des principes essentiels consacrés par la Directive, sans que cette liste ne soit l'exacte reprise des exigences de celle-ci, mais au contraire, soit conçue comme une exigence de remplir les fonctionnalités de la directive tout en laissant aux autorités des pays tiers voire aux entreprises ou autres acteurs concernés un choix très large des moyens.

Le critère de l'effectivité se mesure à trois sous-critères:

- la capacité du système à mettre en place un système effectif d'information des personnes concernées et des responsables des traitements de leurs droits et devoirs;
- l'offre par le système à évaluer, d'un niveau de « support and help to individual data subjects in the exercise of their rights » dont les caractéristiques sont à nouveau décrites de manière fonctionnelle et minimale (rapidité et effectivité des moyens de recours, caractère non prohibitif des coûts d'accès et de recours et transparence du mécanisme de recours);
- le caractère « approprié » du mécanisme de recours.

Nous reviendrons sur la signification de ces critères lors de notre analyse de la compatibilité des articles 25 et 26 avec les principes de l'OMC (infra, n° 14 et ss.)

B. Les exceptions de l'article 26

7. La directive, « sous réserve de dispositions contraires de leur droit national régissant des cas particuliers », édicte certaines exceptions au principe de l'article 25 et autorise ainsi des transferts de données à caractère personnel vers des pays n'offrant pas un niveau de protection adéquat. Deux types d'exception sont prévus: le premier vise certaines catégories de flux; le second vise la substitution à un mode adéquat de protection, d'un mode « ad hoc » de protection: le contrat.

A propos de la première catégorie d'exceptions, l'article 26.1 vise notamment la cas où la personne concernée a indubitablement donné son

consentement à l'opération de transfert (article 26.1a). On ne peut parler de véritable consentement que si celui-ci est « éclairé », c'est-à-dire si la personne concernée a conscience qu'il s'agit bien d'un flux transfrontalier, connaît le pays de destination des informations qu'elle transmet et réalise que ce pays n'assure pas un niveau de protection adéquat des données. D'autres exceptions existent. Elles reprennent les hypothèses prévues par l'article 7 pour légitimer un traitement à l'exception de celle visée à l'article 7f: soit le transfert nécessaire à l'exécution du contrat ou à l'exécution de mesures pré-contractuelles, soit entre la personne concernée et le responsable du traitement, soit entre le responsable du traitement et un tiers dans l'intérêt de la personne concernée, soit le transfert sert à la sauvegarde d'un intérêt vital ou d'intérêt public important ou s'opère dans le cadre d'une action en justice.

On notera qu'il importe que le transfert soit nécessaire au regard de tels intérêts et qu'il ne suffit pas que l'intérêt contractuel existe pour que le transfert soit autorisé. Ainsi, dans le cadre d'une multinationale, la création en terre lointaine d'une banque de données relative à l'ensemble des travailleurs et les flux engendrés à partir des filiales européennes ne pourront bénéficier de l'exception de l'article 26 que si le responsable démontre qu'il existe une nécessité d'opérer ce transfert pour l'exécution du contrat. Sans doute, cette nécessité n'existera que pour quelques employés appelés par exemple à une grande mobilité au sein de la firme et à leur propos uniquement pour quelques données et non pour l'ensemble des données.

8. La seconde catégorie d'exceptions entend substituer à des modes adéquats de protection, ceux palliatifs envisagés par le responsable dans le cadre d'un contrat régissant un flux ou plusieurs flux. Ainsi, si le secteur marketing d'un pays tiers n'offre pas de protection adéquate aux données originairement protégées par la Directive, une ou plusieurs entreprise(s) (voire une association de sociétés de marketing) peut(vent) prendre dans le cadre des contrats couvrant les flux transfrontières en provenance d'Europe, des engagements supplémentaires, par exemple en limitant les finalités de réutilisation des données, ouvrant le droit d'opposition et finalement en permettant à une autorité de protection des données d'inspecter

leurs traitements[11]. A propos de ce second type d'exception, une autorisation de l'Etat membre est nécessaire. Cette autorisation suppose la vérification du caractère « suffisant » des garanties offertes. L'Etat membre informe la Commission de telles autorisations et des oppositions exprimées par d'autres Etats membres sont possibles. On souligne à ce propos, le rôle important joué par la Commission qui peut, après examen de telles mesures palliatives, conclure soit à leur rejet soit à la proposition de mesures supplémentaires. On notera que la Commission peut elle-même proposer des clauses modèles satisfaisant aux exigences de la directive et ce conformément à l'article 26 § 4[12].

Première partie: La protection des données à caractère personnel et l'OMC[13]

A. Des traités conclus dans le cadre de l'OMC et de la vie privée comme exception légitime au principe du libre commerce

12. L'importance croissante de l'organisation mondiale du commerce[14] dans la régulation du commerce international est patente. Depuis l'Uruguay Round, une révision fondamentale du « General Agreement on

11. Historiquement, le premier cas où des dispositions contractuelles ont été considérées par une autorité de contrôle comme offrant une protection adéquate à des données nominatives transférées hors Europe a été le fameux cas « Citybank » qui concernait des données générées par des cartes de crédit distribuées à des utilisateurs des chemins de fer allemands. Sur ces clauses contractuelles et les clauses modèle élaboré par la Chambre de Commerce Internationale, lire E. Longworth, Contractual Privacy Solutions, 22nd Int. Conference On Privacy and Data Protection, Venezia, 27 - 30 sept. 2000 et Y. Poullet, S. Louveaux, V. Perez Asinari, Data Protection and Privacy in Global Networks, 8 EDI Law Review, 2001, 147-196.

12. Le lecteur se référera aux décisions de la Commission relatives aux clauses contractuelles standard, en particulier à la décision du 15 juin 2001 (C (2001)1539, J.O. L 181 du 4 juillet 2001). Pour une analyse critique de ces clauses, lire outre l'article de Poullet, Louveaux et Perez-Asinari, cité supra note 10, B. Wellbery et R. Barcelo, European Commission's Model Contractual clauses: Paving the Way for International Transfers or a New Hurdle, Privacy and Information Law report, Vol.1, 7, 2001, pp. 9 et s.

13. Cette première partie s'appuie largement sur les réflexions de V. Perez-Asinari, « Is there any Room for Privacy and Data Protection within the WTO Rules? », article à paraître in Computer Law & Sec., 2003.

14. Pour une présentation de l'OMC, "What is the WTO?" available at: http://www.wto.org/english/thewto_e/whatis_e/whatis_e.htm.

Tariffs and Trade » a été entreprise; des règles nouvelles ont été édictées pour le commerce des services et sur cette base, des règles spécifiques notamment en matière de propriété intellectuelle (les TRIPS Agreement) et de télécommunications ont été conclues. Un accord sur le règlement des litiges a été adopté[15]. L'ensemble vise, sur une base d'accords nécessairement multilatéraux et globaux, à libéraliser le commerce en créant progressivement les conditions d'un marché global ouvert. Ces accords purement économiques n'imposent aucune condition de respect des droits de l'Homme à l'accession des Etats membres[16]. La participation de l'Union européenne, à côté de celle des Etats membres, a fait l'objet d'un avis substantiel de la Cour de Justice des Communautés européennes le 15 novembre 1994[17].

Dans le cadre des accords conclus au sein de l'OMC, les exceptions à la libre circulation des produits et services sont sévèrement limitées. Les réglementations européennes fondées sur la protection des libertés individuelles, en particulier de leur vie privée, imposent, nous l'avons vu, des limites aux flux transfrontières des données personnelles et sont donc perçues comme une barrière à la libéralisation des échanges.

15. A propos de ces multiples traités, « The multilateral trading system: past, present and future » et « The WTO agreements », documents disponibles sur le site http://www.wto.org/english/thewto_e/whatis_e/inbrief_e/inbr01_e.htm.

16. Avis 1/ 94 de la Cour du 15 novembre 1994, Compétence de la Communauté pour conclure des accords internationaux en matière de services et de protection de la propriété intellectuelle – Procédure de l'article 228, paragraphe 6, du traité CE, Recueil de jurisprudence 1994 page I-05267. « En conséquence, la Cour émet l'avis suivant: 1) La Communauté est seule compétente, au titre de l'article 113 du traité CE, pour conclure les Accords multilatéraux relatifs au commerce des marchandises. 2) La compétence pour conclure le GATS est partagée entre la Communauté et ses Etats membres. 3)La compétence pour conclure les TRIPS Agreements est partagée entre la Communauté et ses Etats membres ». A propos de cet avis controversé, lire Piet Eeckhout « The domestic Legal statusof the WTO Agreement: Interconnecting Legal Systems » Common Market Law Rev. 34: 11-58, 1997 Kluwer Law International "(...) I would argue that one domestic legal status is clearly to be preferred over sixteen" et Pierre Pescatore, "Opinion 1/94 on "Conclusion of the WTO Agreement: Is there an escape from a Programmed Disaster?", Common Market Law Rev., 36: 387-405, 1999, Kluwer Law International. "There were good reasons to have the WTO Agreement signed and accepted jointly by the Community and its Member States, but on grounds totally different from those retained by the Court in Opinion 1/94".

7. A cet égard, not. Th. Fleury et N. Ligneul, « Commerce international, Droits de l'Homme, Mondialisation: Les Droits de l'Homme et l'organisation mondiale du commerce », in Commerce Mondial et Protection des droits de l'Homme, Bruylant, Bruxelles, 2001, pp. 182 et s.

P. Swire et R. Litan résument comme suit les objections[18] adressées à la prise en considération de telles restrictions: « The title of this book: "None of your Business" suggests two ways in which restrictive data protection laws might clash with free trade agreements that have been signed by the United States, the members of the European Union, and most other countries in the world. First, the United States and other non-EU countries may argue that the Directive is an improperly extraterritorial enactment and that it is one of Europe's business to dictate how personal information should be handled outside Europe. Second, there is a suspicion among some that the Directive may serve protectionist goals, saying "None of your business" to non-European companies that face the barrier of having to comply with complex European privacy laws»[19].

13. Ainsi, les craintes de l'utilisation des réglementations européennes "Vie privée" comme mesure protectionniste sont souvent agitées pour dénier leur légitimité dans un monde globalisé fondé sur la libre circulation des biens et services. Au regard de cette crainte, les articles XIV de l'Accord général sur le commerce des services (GATS) et l'article XX de l'Accord général en matière tarifaire et commerciale (GATT) soufflent le chaud et le froid.

En effet, si ces articles, en particulier celui présent dans le GATS, reconnaît que la nécessité d'assurer la conformité avec les réglementations relatives à la protection de la vie privée peuvent justifier l'adoption souveraine par les états signataires de mesures restrictives à la liberté du commerce

18. P. Swire et R. Litan, « None of your Business, World data Flows, Electronic and the European Privacy Directive», Brokkings Inst. Press, Washington D.C., 1998.

19. De manière plus agressive encore, la déclaration de I. Magaziner, alors responsable sous la présidence Clinton des négociations avec l'Europe en matière de commerce électronique, lors de la réunion ministérielle d'Ottawa du 9 octobre 1998: « (US should) challenge EU privacy rules under the theory that they represent barrier to trade ».

international[20], cet article insiste sur la nécessité, d'une part, d'une application de ces règles de manière discriminatoire ou de manière à constituer une restriction déguisée à la libre circulation des services et, d'autre part, de non-cohérence des règles avec les dispositions de cet accord[21].

Il importe donc de s'interroger sur la compatibilité des mesures prises par ou en exécution de la directive 95/46 au regard des textes de l'Organi-

20. A cet égard, la déclaration très nette figurant sur le site de l'OMC en réponse à la crainte exprimée par R. Nader sur les riques de voir l'OMC forcer les Etats signataires à renoncer à leur protection de la vie privée: « Following a speech on the need for protection of on-line consumers, made in Washington on 9 January 2001, Mr. Raph Nader was quoted as saying that « particularly in the area of internet privacy protections, the WTO is forcing governments to forego sovereign privacy protections deemed to be overly restrictive to international trade ». This is difficult to understand. No decision or action on the protection of Internet privacy has ever been taken in the WTO. Far from "forcing governments to forego sovereign privacy protections" (which it would have no power to do in any case), the WTO has had nothing whatever to do with Internet Privacy. Moreover, a safeguard for individual privacy is built into the framework of the GATS itself. One of the General Exceptions in Article XIV of the GATS, overriding all other provisions, covers measures Governments might find iy necessary to take for "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts". (GATS: Fact and Fiction. Misunderstandings and scare stories: The WTO and Internet Privacy, texte disponible sur le site http://www.wto.org/english/tratop_e/serv_e/gats_factfiction10_e.htm). A noter sur le même site, la réponse à l'article de Mr. M. Dobbin, journaliste canadien, qui dénonçait le rôle négatif de l'OMC, vis-à-vis des législations nationales protectrices de l'environnement.

21. Le texte est libellé comme suit: "General Exceptions: Subject to the requirement that such measures are not supplied and applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguished restriction on trade in services, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures.
(a) necessary to protect public morals or to maintain public order
(b) necessary to protect human, animal or plant life or health
(c) necessary to secure compliance with law or regulations which are not inconsistent with the provisions of this Agreement those relating to:
(i) the prevention of deceptive and fraudulent practices or to deal with the effects of a default on services contracts;
(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts;
(iii)safety. »
Une disposition quasi-similaire figure dans le GATT (article 20). Elle ne fait cependant pas mention à la question de la vie privée, ce qui est normal vu l'objet même de cet accord restreint aux produits industriels ou manufacturés.

sation Mondiale du Commerce[22]. Cette interrogation et la réponse à celle-ci sont d'autant plus urgentes que le 14 novembre 2001, lors de la conférence interministérielle de l'OMC à DOHA, la déclaration ministérielle finale incluait parmi les sujets de négociation pour le prochain « round » la question de la vie privée[23].

B. Les articles 4, 25 et 26 de la directive européenne et leurs applications sont-elles compatibles avec le traité de l'OMC?

14. La jurisprudence des panels mis en place par l'OMC pour juger des conflits au sein de l'OMC a eu l'occasion à quelques reprises d'analyser le bien-fondé de décisions nationales restrictives pour le commerce international au regard notamment des articles XIV du GATS ou XX du GATT[24].

Certains critères permettent de juger de ce bien-fondé.[25]

Le « necessity test » ou test de « l'important apport »

15. Ainsi, le premier critère est indiscutablement le « necessity test », c'est-à-dire selon l'expression du WTO Working Party on Domestic Regulation, « The requirement that regulatory measures be no more trade restrictive than necessary – is the means by which an effort is made to balance

22. Sur le GATT et plus généralement l'OMC, lire JJ. Rey et J. Dutry, « Institutions économiques internationales », 3e édition, Bruylant, Bruxelles 2001; J-H. Jackson, The World Trading System: Law and Policy of International Economic Relations, Cambridge, MIT Press, 2e Edition, 1997, 441 pages; «WTO Dispute Settlement Practice relating to the GATS », JIEL, 1999, pp. 295-346.

23. WTO Ministerial declaration adopted le 14 novembre 2001, disponible sur le site de l'OMC déjà cité.

24. Sur ces exceptions, lire Bal Salamn, «Free Trade Agreements and Human Rights: Reinterpreting Art XX of the GATT », Minessota Journ of Global Trade, 10(2001)1, 62-108; C. Beven, «The WTO and its interpretation of the Art. XX exceptions», Georgia Law Journ. of Int. and Comp. Law 20(2000), 1, 181-202,

25. Les clauses introductives de l'article XX du GATT 1994 interdisent l'application d'une mesure qui bien que relevant de l'une des dix exceptions énumérées par l'article XX constituerait:
- une « discrimination arbitraire » (entre les pays où les mêmes conditions existent);
- une « discrimination injustifiable »(dans la même situation que ci-dessus);
- une « restriction déguisée au commerce international ».

(T. Fleury, « L'organisation mondiale du Commerce», Bruylant, Bruxelles, 1999, p. 56 et s. Cf. l'analyse à cet égard de l'affaire « Etats-Unis - Normes concernant l'essence et ancienne formule » (20 mai 1996 (WT/DS2R et WT/DS2/AB/R)).

between two potentially conficting priorities: promoting trade expansion versus protecting the regulatory rights of governments »[26].

Par là, le Working Party rappelle le principe général de proportionnalité[27] qui exige une balance d'intérêts entre des valeurs contradictoires: l'intérêt du libre commerce et la défense par les Etats de la vie privée de leurs citoyens. Par ailleurs, comme l'affirme le panel dans l'affaire Korea-Measures Affecting Imports of Fresh, Chilled and Frozen Beef[28], le critère de nécessité ne doit pas être pris au sens strict: « ce qui est inévitable », mais de manière plus large, comme ce qui apporte une « contribution importante » (et non une simple contribution) à la réalisation des objectifs poursuivis par la réglementation[29].

26. Working Party on Domestic Regulation, "Application of the necessity test: issues for consideration", 8 October 1999, Job N° 5929, Informal note by the Secretariat. Available at: http://www.wto.org.english/tratop_e/serv_reg_secretariatnot_e.htm.

27. Sur ce principe, la remarquable thèse publiée récemment de S. van Drooghenbroek, « La proportionnalité dans le droit de la convention européenne des droits de l'Homme», Bruylant, Publications FUSL, Bruxelles, 2002.

28. « Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef », WTO, Report of the Appellate Body, 11 December 2000, (WT/DS161/AB/R – WT/DS169/AB/R), available at: http://www.worldtradelaw.net/:"(...) The Panel was established to consider a complaint by Australia and the United States with respect to Korean measures that affect the importation of certain beef products. The aspects of these measures relevant for this appeal relate to, first, domestic support provided to the beef industry and to the Korean agriculture sector more generally and, second, the separate retail distribution channels that exist for certain imported and domestic beef products (...)». Le lecteur trouvera l'ensemble des textes des décisions jurisprudentielles et leur analyse in GATT/OMC, Recueil des contentieux du 1er janvier 1948 au 31 déc., 1992, E. Canal-Forgues – T. Fleury (Dir.), Bruylant, Bruxelles, 2001.

29. A cet égard, les attendus suivants: "161. We believe that, as used in the context of article XX(d), the reach of the word 'necessary' is not limited to that which is indispensable' or 'absolute necessity' or 'inevitable'. Measures which are indispensable or of absolute necessity or inevitable to secure compliance certainly fulfill the requirements of Article XX(d). But other measures, too, may fall within the ambit of this exception. As used in Article XX(d) the term 'necessary' refers, in our view, to a range of degrees of necessity. At one end of this continuum lies 'necessity' understood as 'indispensable': at the other end, is 'necessary' taken to mean is, in the continuum, located significantly closer to the pole of 'indispensable' than to the opposite pole of simple 'making a contribution to'".
"164. In sum, determination of whether a measure, which not 'indispensable', may nevertheless be 'necessary' within the contemplation of Article XX(d) involves in every case a process of weighing and balancing a series of factors which prominently include the contribution made by the compliance measure to the enforcement of the law or regulation at issue, the importance of the common interests or value protected by the law or regulation, and the accompanying impact of the law or regulation on imports or exports".

16. Au regard de cette première condition, que dire des articles 25 et 26 et de leur application? A propos de l'article 25, on notera que le document de base relatif à l'évaluation du critère de la protection adéquate[30] commence par une analyse des risques encourus par les personnes concernées du fait de la transmission des données vers les pays tiers et déduit de cette analyse[31] des critères de « conformité » et d' « effectivité » du système dont le caractère adéquat doit être évalué non en principe mais au regard des risques particuliers révélés par les circonstances de transfert[32]. Ces critères ont été systématiquement appliqués dans les analyses auxquelles la Commission s'est livrée dans les cas où elle a dû juger du caractère adéquat des systèmes qui lui étaient soumis.

Le critère de la « conformité » s'adresse au contenu de la protection accordée aux personnes concernées (principe de l'accès, des données sensibles, de la détermination des finalités, etc.). Il reprend une liste des principes essentiels consacrés par la Directive, sans que cette liste ne soit l'exacte reprise des exigences de celles-ci, mais au contraire, soit conçue comme une exigence de remplir les fonctionnalités de la directive tout en laissant aux autorités des pays tiers voire aux entreprises ou autres acteurs concernés un choix très large des moyens.

Le critère de l'effectivité se mesure, nous l'avons dit (supra, n°6), à trois sous-critères:

- La capacité du système à offrir un bon respect de ses règles, en particulier par une information effective des responsables des traitements et des personnes concernées de leurs droits et devoirs;

30. «First Guidelines concerning transfers of Personal Data to third countries. Possible means of evaluating the adequate nature of Protection », Discussion Paper adopté par le Groupe dit de l'article 29 le 26 juin 1997, DG XV D/5020/97-Fr-final.

31. A ce propos, outre le document cité à la note précédente et l'Opinion 7/99 du 3 décembre 1999 (WP 27) émise par le groupe de travail de l'article 29 à propos des US « Safe Harbor Principles », on lira l'étude élaborée pour la DG XV par Y. Poullet et B. Havelange, Elaboration of a Methodology to evaluate the Adequacy of the Level of the Protection of the Individuals vis-à-vis the Processing of personal Data in Third Countries (European Commission, Official Publications, Office, ISBN 92-828-4304, 1998), qui a servi de base à l'élaboration des critères repris par le Groupe de Travail dit de l'article 29.

32. « Le risque est un événement dommageable dont la survenance n'est pas certaine mais entraîne pour la personne fichée, un dommage. Dans le cadre de transferts de données personnelles, nous avons classifié les risques en quatre grandes catégories ...: les risques de perte de contrôle, de réutilisation de données, de manque de proportionnalité et d'inexactitude de ces données », Y. Poullet, B. Havelange, M-H. Boulanger et A. Lefebvre, op.cit..

- L'offre par le système à évaluer, d'un niveau de « support and help to individual data subjects in the exercise of their rights » dont les caractéristiques sont à nouveau décrites de manière fonctionnelle et minimale (rapidité et effectivité des moyens de recours, caractères non prohibitif des coûts d'accès et de recours et transparence du mécanisme de recours);
- Le caractère « approprié » du mécanisme de recours.

17. Il est remarquable que lors de son analyse de l'interprétation de l'article 26 § 2 à propos des clauses contractuelles[33], les mêmes exigences fonctionnelles aient été retenues pour en déduire le contenu même des clauses contractuelles modèles[34].
Par ailleurs, lorsque la nature du flux comporte en soi les garanties nécessaires à la protection des données, en particulier lorsque le consentement au flux est indubitable, l'article 26 § 1 estime non nécessaire les autres moyens que constitue la protection adéquate par le système du pays tiers ou par les clauses contractuelles.

En d'autres termes, conformément aux textes fondateurs de l'OMC et en particulier au test dit de nécessité que la jurisprudence des panels mis en place par l'OMC met en lumière, c'est au regard des préoccupations importantes qui fondent la directive et dans la mesure où les circonstances du flux transfrontières avivent ces préoccupations que se justifient et la variété et l'intensité des mesures répertoriées par les articles 25 et 26. En aucune manière, la réglementation des pays membres de l'Union européenne ne peut justifier de soi l'interdiction d'un flux. C'est à la lumière des risques concrets que représente un flux que doit s'évaluer le respect des principes essentiels de la directive, étant entendu qu'il existe divers moyens de répondre à ces risques comme il sera développé ci dessous avec l'analyse du second test.

33. Working Group Article 29, Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries, DGXV, D/5005/98 final, W.P. 9.

34. Model Contract to ensure equivalent protection in the context of transborder data flows with explanatory report", 15th ofJune 2001, disponible sur le site http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp46en.pdf

b. Le test de la « non-alternative »

18. Le test de « nécessité » suppose également que soient évaluées l'inexistence ou l'inapplicabilité de toute mesure alternative moins restrictive. La jurisprudence « Measures Affecting Asbestos and Asbestos Containing Products »[35] est intéressante à cet égard. Dans l'affaire, le Canada reprochait à la France le fait que cette dernière imposait un système de contrôle a priori de certains produits et non un système de « controlled use » a posteriori, comme l'imposait le Canada.

Le Panel estima qu'au regard du niveau de protection librement choisi par la France, le système canadien ne présentait pas une alternative suffisante. Pour ce faire, le Panel s'appuie sur le rapport préalable d'experts[36].

Par contre, dans l'affaire « Thailand-Restriction on Importation of and Internal Taxes on Cigarettes », un autre Panel a considéré le 7 novembre 1990[37] que la protection de la santé et la lutte contre le tabagisme, objectifs légitimes poursuivis par la Thailande, pouvaient être atteints par d'autres voies que celle de la prohibition de toute importation de cigarettes, mesure précisément retenue par ce dernier pays. L'autonomie de choix des moyens laissée aux Etats membres de l'OMC[38] ne peut aller jusqu'à

35. « European Communities-Measures Affecting Asbestos and Asbestos-Containing Products », WTO, Report of the Appellate Body, 12 March 2001, (WT/DS135/AB/R), available at: http://www.worldtrade law.net/: "The Panel was established to consider claims made by Canada regarding French Decree No. 96-1133 concerning asbestos and products containing asbestos (décret relatif à l'interdiction de l'amiante, pris en application du code de travail et du code de la consommation) (...)".

36. « 174. In our view, France could not reasonably be expected to employ any alternative measure if that measure would, in effect, prevent France from achieving its chosen level of health protection. On the basis of the scientific evidence before it, the panel found that, in general, the efficacy of 'controlled use' remains to be demonstrated. Moreover, even in cases where 'controlled use' practices are applied 'with greater certainty', the scientific evidence suggests that the level of exposure can, in some circumstances, still be high enough for the re to be a 'significant residual risk of developing asbestos-related diseases (...)».

37. Affaire DS10/R –375/200, texte disponible sur le site http://www.worldtradelaw.net/ « 81. In sum, the Panel considered that there were various measures consistent with the general Agreement which were reasonably available to Thailand to control the quality and quantity of cigarettes smoked and which, taken together, could achieve the health policy goals that the Thai government purses by restricting the importation of cigarettes inconsistently with Article XI: 1.

38. Sur cette autonomie, lire la décision "United States- Standards for Reformulated and Conventional Gasoline", WTO, Report of the Appelate Body, 29 avril 1996 (Affaire DS2/AB/R).

interdire des restrictions aux importations de produits ou services alors que d'autres moyens moins restrictifs permettent d'atteindre le même but.

19. A propos de cette seconde exigence, la législation européenne visée, à savoir les articles 25 et 26 de la Directive 95/46, est remarquable. L'entreprise étrangère voire le pays étranger a le choix de divers moyens pour rencontrer les objectifs de protection des données jugés essentiels par l'Union européenne. Ainsi, la mise sur pied sectorielle voire au niveau d'une seule entreprise d'un système de protection adéquat n'implique en aucune manière le choix du système législatif de protection privilégié en Europe sur le plan interne. L'adoption des « Safe Harbor Principles » comme mode adéquat de protection illustre à suffisance cette ouverture d'esprit européenne qui peut reconnaître l'autorégulation ou la co-régulation[39] comme digne d'offrir cette protection adéquate. Au-delà, l'article 26 § 2 permet aux entreprises, qui ne pourraient se référer à un système de protection adéquat, de l'élaborer grâce à des clauses contractuelles pour lesquelles les contrats modèles proposés par l'Union européenne constituent une référence sans exclure des constructions originales.

Les alternatives mises en place par le texte de la directive témoignent que loin de constituer un diktat – ce qui constituerait à l'évidence la manifestation d'un impérialisme réglementaire européen[40] inadmissible – la solution européenne est ouverte à la prise en considération d'autres appro-

39. Sur cette notion, lire entre autres, T. Fenoulhet, «La co-régulation: une piste pour la régulation de la Société de l'information? », Revue du marché commun et de l'Union européenne, octobre 2001. Selon l'auteur, il s'agit d'une « méthode de régulation comportant trois éléments clés:
- le processus d'élaboration des règles et de développement du consensus entre les parties intéressées;
- l'organisme en charge de la mise en application des règles détenant un pouvoir de sanction (« le Watchdog »);
- le législateur qui encadre la co-régulation et lui donne une validité juridique via un acte législatif.

Pour un aperçu complet des divers modes de régulation: autorégulation, co-régulation et autres formes d'intervention réglementaire de même que leurs interactions, le lecteur se référera à l'ouvrage collectif publié suite à un séminaire sur ce thème tenu à Namur, les 15 et 16 juin 2001: « Gouvernance de la société de l'information » (J.Berleur – C. Lazaro- R. Queck éd.), Cahier du Crid n°22, Bruylant, Bruxelles, 2002.

40. « L'objectif de la directive n'est en effet pas d'exporter son modèle réglementaire hors de ses frontières; son but, au contraire, est de protéger les données des personnes bénéficiant de la protection de la directive, y compris lorsque celles-ci sont envoyées à l'étranger» (Poullet, Havelange, Boulanger et Lefebvre, op.cit.).

ches moins lourdes que celles privilégiées par l'Europe et plus en accord avec les cultures et les systèmes juridiques d'autres pays[41].

c. Le test de la « non-discrimination »

20. Ce test a une double signification: l'une examine la réglementation interne du pays qui se prévaut de l'exception au regard des restrictions imposées aux produits ou services étrangers. Il va de soi qu'il serait contraire aux accords conclus au sein de l'OMC qu'un Etat membre soit plus sévère vis-à-vis de ressortissants étrangers que vis-à-vis de ses propres nationaux. Ce premier test exige que les Etats membres fassent respecter de manière interne et effective les contenus des législations qui fondent des restrictions au commerce extérieur[42].

A cet égard, les pays membres de l'Union européenne argueront à juste titre du fait que l'article 6 du Traité de l'Union européenne[43], la Charte européenne des droits de l'Homme, signée à Nice[44] et la signature de la convention européenne des Droits de l'Homme[45] imposent aux pays membres, le contrôle par les Cours tant de Luxembourg que de Strasbourg leur respect en droit interne des droits fondamentaux, en particulier de la vie privée sous ses divers aspects énumérés tant par la directive 95/46 que celle récemment adoptée en matière de vie privée dans le secteur des communications électroniques. Ces pays ajouteront que la directive met en place avec l'autorité de contrôle (article 28) et les principes du recours juridictionnel, les moyens de garantir l'effectivité du respect des garanties énoncées par le texte.

41. C'est ce que notre rapport appelait le coefficient « différence culturelle ». Sur cette notion, cf. Y. Poullet, « La protection adéquate dans les flux transfrontières de données », 19th Conférence Internationale des Commissaires à la Protection des Données, Bruxelles, 17-19 septembre 1997, pp. 2 et s.

42. Dans l'affaire des cigarettes thaïlandaises, le Panel note que « therefore that Thailand's practice of permitting the sale of domestic cigarettes while not permitting the importation of foreign cigarettes was an inconsistency with General Agreement not 'necessary' within the meaning of Article XX(b) ». Dans le même sens, l'affaire déjà citée "Etats-Unis: Normes concernant l'essence nouvelle et ancienne formules" du 20 mai 1996 où les Etats-Unis avaient soumis les seules essences importées à des normes plus lourdes.

43. Sur cette disposition, cf. infra n° 32.

44. Sur la charte et sa valeur obligatoire, cf. infra n° 34.

45. Sur les obligations découlant pour les Etats européens de leur signature de la Convention européenne des droits de l'Homme, cf. infra n° 36.

L'Union européenne, s'est engagée par l'article 286 CE[46] à respecter les principes de la directive: « à partir du 1er janvier 1999, les actes communautaires relatifs à la protection des données à caractère personnel et à la libre circulation de ces données sont applicables aux institutions et organes institués par le présent Traité ou sur la base de celui-ci ». La création d'une autorité constitue le moyen d'assurer au niveau des organes communautaires cette fois, cette même protection.

21. La seconde signification du test commande que les divers pays externes soient soumis de manière égale aux mêmes restrictions, bref qu'un pays ne soit pas avantagé vis-à-vis d'un autre[47]. Il s'agit là d'une application du principe de non-discrimination, principe contenu dans l'article II du GATS: « 1. With respect to any measure covered by this Agreement, each Member shall accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favorable than it accords to like services and services suppliers of any other country".

A cet égard, il pourrait être argué que l'entreprise suisse ou canadienne qui doit se soumettre à une législation en matière de protection des données, se trouve dans une situation moins favorable que celle américaine, bénéficiant du système plus souple du Safe Harbor ou de celle coréenne qui se satisfait de simples clauses contractuelles. Cette objection ne résiste pas à l'analyse dans la mesure où le critère commun est dans tous les cas le caractère « adéquat » de la protection offerte. Si le concept de protection adéquate est ouvert – et nous avons montré combien cette approche ouverte était respectueuse du traité de l'OMC et du test des mesures alternatives[48] en renvoyant à une diversité de moyens pour réaliser cet objectif unique –, le contrôle de son existence et de son respect s'opère selon une

46. Sur cet article, lire le commentaire de A. Meyer-Heinse, « Réalité et perspectives du droit communautaire des droits fondamentaux», F. Sudre et H. Labayle (dir.), Coll. Droit et Justice, Bruylant, Bruxelles, 2000, p. et F. Maioni, « Le cadre réglementaire des traitements de données personnelles effectuées au sein de l'Union européenne», RTD eur. 38(2), 2002, avril-juin.

47. Sur cette nécessité de non-discrimination, G.Schafter, « Globalization and Social Protection: the Impact of E.U. and Information Privacy Rules in Ratcheting up of U.S. Privacy Standards», 25 Yale Journ. Int'l L. Rev. 1 (2000),p.50.
J. Reidenberg, « The Globalization of Privacy: the Movement towards obligatory Standards for Information Practices », in Visions of privacy, Policy Choices for the Digital age, 6 (C. Bennett and R. Grant (ed.), 1999, p.219-220: « Any European decision ...must thus satisfy the test of non discrimination».

48. Cf. supra n°20.

grille qui oblige à analyser les divers systèmes proposés comme adéquats selon les mêmes critères qui ont été définis par le Groupe de l'article 29 et ratifiés par le groupe de l'article 31 mis en place par la directive 95/46[49]. Ces critères servent de référence unique pour apprécier la protection offerte par des mesures contractuelles ou par un système réglementaire qu'il s'agisse d'auto-réglementations, de normes techniques ou de réglementations législatives ou gouvernementales, qu'il s'agisse de réglementations sectorielles, de privacy policies d'une entreprise ou de réglementations dites omnibus.

Sans doute, la connaissance de cet environnement n'est pas chose aisée et surtout la signification protectrice des textes est-elle une question non seulement de contenu mais également de pratiques administratives judiciaires voire des entreprises. Prenons le critère du recours aisé et des sanctions existantes, proportionnées et au moins dissuasives, un des critères importants d'effectivité souligné par les textes européens qui fixent la méthodologie d'analyse des flux transfrontières[50], le respect de ce critère dans le cadre du système des « Safe Harbor Principles » a fait l'objet de nombreuses analyses et de demandes d'explicitation auprès des experts américains. Si les « Safe Harbor Principles » ont sur ce point été reconnus comme répondant à l'objectif européen, c'est dans la mesure où l'effectivité des Principles repose en grande partie sur les garanties qu'apporte complémentairement la législation américaine[51] sur les « False et deceiptive Statements ». Le Statement émis par l'entreprise et en son sein par un responsable personne physique et exigé par les « Principles » prend, grâce à cette législation placée sous le contrôle de la Federal Trade Commission

49. Cf. à cet égard, l'attendu n°4 de la décision de la Commission du 26 juillet 2000 relative à l'adéquation de la protection offerte par les Safe Harbor Privacy Principles et les questions fréquemment posées, disponible sur le site http://europa.eu.int/comm/internal_market/fr/dataprot/news/decision.pdf.
A noter en outre l'avis que le Groupe de travail institué par l'article 29 peut émettre d'initiative sur le niveau adéquat offert par un pays tiers et le rapport annuel que ce même groupe de travail doit émettre, selon l'article 30 . 1. b)

50. En particulier le document de travail n°12 adopté le 24 juillet 1998: « Transferts de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive communautaire sur la protection des données ».

51. .... qui n'a pas d'équivalent dans les pays européens.

(FTC), une signification protectrice pour les personnes concernées[52] que ne pourrait avoir la même déclaration dans nos systèmes européens.

En d'autres termes, c'est au regard des particularités de chaque système étranger qui doit être pris dans son ensemble et compte tenu du fonctionnement interne de ce système étranger, que s'effectue, sans discrimination, l'examen du caractère adéquat de la protection offerte. Cet examen peut être effectué a priori au niveau européen et non de chaque Etat membre, vu les compétences octroyées sur ce point par l'article 25, 3, 4 et 6, dispositions qui obligent les Etats membres à informer la Commission des décisions prises à ce propos et en outre permet à la Commission de prendre des décisions positives ou négatives sur le caractère adéquat d'un système étranger et par l'article 26 qui autorise l'élaboration par la Commission de clauses modèles[53]. Il peut également être le fait d'organes nationaux selon des procédures qui peuvent être plus ou moins lourdes et selon des appréciations plus ou moins sévères du caractère adéquat. Sans doute, à ce niveau, pourrait-on craindre des applications discriminatoires.

Conclusion

22. Notre conviction, aux termes de cette analyse, est que la signature des accords conclus par l'Union européenne et les Etats membres du fait de leur participation à l'OMC ne leur interdit pas, bien au contraire, de se prévaloir des mesures susceptibles d'être prises dans le cadre des articles 4, 25 et 26 de la directive dans la mesure où l'application de ces articles garantit des mesures « nécessaires », « non discriminantes » et que leur éventail laisse à chaque Etat et aux entreprises la possibilité d'alternatives quant au choix du mode de protection, alternatives plus conformes à leur système et traditions juridiques.

Cette réflexion n'exclut pas une critique fondamentale au système mis en place par l'OMC. Les exceptions relatives à la « privacy » comme à d'autres intérêts publics ou jugés essentiels (la sécurité, l'environnement, la santé) sont certes prévues mais les préoccupations que ces exceptions

...qui peut ainsi bénéficier de la « class action » inconnue dans nos droits européens, de « punitive damages », d'une procédure rapide et accessible, etc.
Sur l'analyse des clauses modèle proposées par la Commission et leur comparaison avec les clauses dites CCI, lire Y. Poullet, S.Louveaux et M. V. Perez-Asinari, « Data Protection and Privacy in Global Networks: A European Approach», 8 EDI Law Review, 2001, 147-196.

expriment sont bien externes aux objectifs de l'OMC. Il y a dissociation entre les règles du commerce et celles des Droits de l'Homme. Les normes relatives à ces deux mondes ne se rencontrent pas si ce n'est exceptionnellement, en cas de conflits entre elles et sous la forme alors d'une exception dont il s'agira de justifier l'exhibition.

Nombre d'auteurs[54] ont déploré cette césure. Cette dissociation explique peut-être la difficulté à résoudre d'éventuels conflits entre droits du commerce et droits de l'Homme, nés de l'enchevêtrement entre des ensembles normatifs d'abord conçus comme des ensembles autonomes.

Or, cette dissociation nie l'interdépendance des droits économiques et des droits de l'Homme, entre les droits de l'Homme et le commerce international[55].

23. A cet égard, Th. Fleury et N. Ligneul[56] plaident pour une reconnaissance des droits de l'homme dans le droit du commerce international. « L'appréhension des droits de l'homme par l'Organisation mondiale du commerce aurait donc pu être d'une nature différente s'ils sont entendus comme les droits de l'homme en tant que citoyen ou en tant qu'agent économique. En se fondant sur l'universalité des droits de l'homme, l'OMC aurait pu attraire cette matière à sa compétence, ou alors, elle aurait pu ne se déclarer compétente que pour défendre les droits de l'homme qui ont un lien avec le commerce, à savoir les droits de l'homme en tant qu'agent économique. Elle n'a fait ni l'un ni l'autre: la voie qui a été suivie est celle du refus de reconnaître une valeur au concept universel des droits de l'homme autant qu'à celui des droits de l'homme en tant qu'agent économique ».

54. Cf. not. B. Brantner et A. Rosas, « Préférences commerciales et Droits de l'Homme» in L'Union européenne et les Droits de l'Homme, Ph. Alston (éd.), Bruylant, Bruxelles, 2001, p. 736 et 737, etc.

55. Sur la nécessité d'une interdépendance de ces deux valeurs, lire J. Reidenberg, Rules of the Road for global electronic Highways: merging the Trade and Technical Paradigms, 6 Harv. Journal of Law and Technology, 1993, p.290 et 291 précisément à propos des règles relatives aux flux transfrontières relatives à la protection des données, règles adoptées dans certains états européens dès avant la directive.

56. T. Fleury - N. Ligneul, « Commerce international, Droits de l'homme et l'Organisation mondiale du commerce», in Commerce mondial et Protection des droits de l'homme, Bruylant, Bruxelles, 2001, p. 180.

Deuxième partie: Le droit et le devoir des Etats membres de l'Union européenne et des Etats membres de veiller au respect de la protection des données dans le commerce mondial

24. La première partie se concevait comme une démonstration négative. Les instruments dont la directive dote les Etats membres en matière de flux transfrontières ne sont pas incompatibles avec les engagements internationaux pris par l'Union européenne en matière de commerce international, en particulier dans le cadre de l'OMC.

La seconde partie de l'exposé vise à justifier, positivement cette fois, l'obligation des Etats membres et de l'Union à militer sur le plan international pour garantir aux personnes protégées par la Directive, la protection effective de leur vie privée.

La démonstration suivra le cheminement suivant:

- A l'inverse des Etats-Unis, la protection de la vie privée au sens large est considérée non comme une simple prérogative de droit privé mais comme un « droit fondamental », protégé par l'ordre juridique communautaire.
- Ce droit fondamental, consacré tant par la Convention européenne des Droits de l'Homme que par le Traité de Rome, fait partie d'un « ordre public communautaire ». Les Etats membres et l'Union européenne ont donc souscrit à des obligations à caractère objectif, obligations de vigilance et de « due diligence » de veiller à son respect.
- Cette même obligation entraîne, sur le plan international cette fois, une responsabilité internationale des Etats membres même lorsqu'ils sont parties à des traités internationaux, en cas d'abstention de la part de ses Etats membres alors même que des violations des droits fondamentaux sont constatées.

A. La protection de la vie privée: l'approche européenne versus l'approche américaine

25. Nombre d'auteurs[57] soulignent la convergence de toutes les nations démocratiques, en particulier, nord-américaines et européennes autour des mêmes principes de base en matière de protection des données[58] et leur adoption d'une définition commune de la « privacy » comme « droit à l'autodétermination ». Les discours officiels tant aux Etats-Unis qu'en Europe[59] soulignent l'importance critique de la protection des données pour assurer le développement de la société de l'information.

La distinction ne se situe donc pas au niveau des principes mais du statut qu'on reconnaît à ces principes de base. Carter Manny[60] résume comme suit cette différence d'approche: « When European state that privacy is a fundamental right, the effect among Americans is to frame questions of consumer information privacy in terms of privacy interests of individuals competing against organisational or societal interests ». Joel Reidenberg[61] est plus net encore: « The Background and underlying philosophy of the European Directive differs from that of the United States. While there is a consensus among democratic society that information privacy is a critical element of civil society, the U.S has, in recent years, left the protection of privacy to markets rather than law. In contrast, Europe treats privacy as a political imperative anchored in fundamental human rights». Sans doute, la réflexion devrait être sur ce point approfondie.

57. A cet égard, notamment J. Reidenberg, « Resolving conflicting International Data Privacy rules in Cyberspace», 52, Standford Law Review (2000), 1322 et s.; C. Bennett et R. Grant, "Introduction", in Visions of Privacy: Policy choices for the Digital Age», 1999, p. 6 et s.; P.M. Schwarz, « Privacy and Democracy in Cyberspace», 52 Vand. L. Review (1999), 1663-1665; C. Manny, « European and American Privacy Commerce, Rights and Justice», to be published in the Proceedings of the Academy for Legal Studies in Business Conference, Albuquerque, New Mexico, Aug. 2001. Cf également dès 1980 dans le cadre des travaux de l'OCDE, la déclaration de M. Kirby, TBDF and the « Basic Rules of Data Privacy », 16 Stan. J. Int. Law Review (1980), p. 27: « Surprisingly, in all the major international efforts that have so far addressed ... (data protection), there has been a broad measure of agreement on the "basic rules" around which domestic privacy legislation should cluster».

58. A cet égard, C. Bennett, « Regulating Privacy Data Protection and Practice Policy in Europe and the United States», 1992, p. 95-115.

59. Ainsi, sous le gouvernement Clinton, l'importante déclaration: The White House, A Framework for Global Electronic Commerce, 1er juillet 1997, p. 13 et 14 (disponible sur le site http: www.ecommerce.gov/framework.htm.) plaidant pour la reconnaissance de l'importance de la protection des données comme condition du développement d'Internet.

60. C.H. Manny, art. cité, p. 12.

61. J. Reidenberg, « E-commerce and Trans-Atlantic Privacy, 38 Houston Law Review», 2001, p.731.

26. Cette reconnaissance en Europe du droit à la vie privée comme « droit fondamental » ne modifie pas le contenu de la protection. Que ce soit aux Etats-Unis ou en Europe, la protection s'entend d'une démarche procédurale plus que substantielle[62]. La convention européenne des Droits de l'Homme et la Directive, à l'instar des « Fair Principles of Informational Privacy » chers à l'approche américaine, ne définissent point la « vie privée » mais mettent en place des standards procéduraux aptes à prévenir des atteintes à cette vie privée dont la notion loin d'être univoque, renvoie au contraire à la protection de l'ensemble des libertés: celle de se déplacer, celle d'obtenir un crédit ou un emploi, celle de s'exprimer ou de communiquer librement et de ne point subir de discrimination. Bref, la vie privée n'est pas une liberté supplémentaire mais elle apparaît comme la condition de toutes les autres.

La reconnaissance de la « vie privée » comme droit fondamental et non comme simple défense d'intérêts donne cependant aux « standards » mis en place une valeur juridique autonome « objective », c'est-à-dire non soumis à la pure discrétion, non seulement des parties – que leurs volontés s'expriment dans un contrat ou une auto-réglementation –, mais également de l'Etat lui-même. « L'étude attentive de la jurisprudence des organes de Strasbourg montre que les droits fondamentaux garantis par la Convention ne sont pas seulement des droits subjectifs ayant pour fonction de protéger l'individu contre les ingérences des pouvoirs publics (et privés) mais qu'ils peuvent remplir également une fonction objective[63]: ces droits font alors office, selon le professeur Malinverni[64] de « principes directeurs de toute

62. Sur cette affirmation, lire J. Dhont et M-V. Perez Asinari, «Regulating Data Protection in a Cross-Cultural Perspective», article en cours de publication réalisé dans le cadre d'une étude menée par le CRID pour le Fonds de la recherche de la Communauté française de Belgique.

63. Sur le caractère « objectif » des Droits de l'Homme, lire not. J-F. Renucci, «Droit européen des Droits de l'Homme», 2e édition, LGDJ, Paris, 2001, n° 23, p. 28; K. Vasak, «Vers un droit international spécifique des droits de l'Homme», in Les dimensions internationales des droits de l'Homme, Unesco, 1978, p. 707 et s.

64. G. Malinverni, «Les fonctions des droits fondamentaux dans la jurisprudence de la Commission et de la Cour européenne des droits de l'Homme», Im Dienst an der Gemeinschaft, Helbing et Lichtenhahn, 1989, 542.

activité de l'Etat » et « ils doivent orienter l'action de l'ensemble de ses organes et imprégner de leurs valeurs tout son ordre juridique[65] ».

27. Il s'agit bien, comme le note l'article 6 du Traité de l'Union européenne, d'assurer « la prééminence des droits fondamentaux en tant que valeurs sociales sur l'Etat »[66]: « L'Union européenne respecte les droits fondamentaux tels qu'ils sont garantis par la Convention européenne de sauvegarde des Droits de l'Homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, et tels qu'ils résultent des traditions constitutionnelles communes aux Etats membres, en tant que principes généraux du droit communautaire ». Cette reconnaissance fondamentale du droit à la vie privée comme droit de l'Homme induit non seulement des limites constitutionnelles à l'action de l'Etat ...et, selon la Charte européenne, à l'action des pouvoirs privés mais en outre fonde un devoir de l'Etat. Une telle approche différencie fondamentalement l'approche européenne de l'approche américaine comme le note C. Leben[67]: « Mais à la différence de son homologue (américain)[68] dont l'implantation indépendante outre Atlantique remonte à la même époque, l'Europe, avec des variations selon les pays, n'a jamais renoncé à l'action continue de l'Etat, i.e. du gouvernement, qui est certes l'entité contre laquelle la protection des droits est organisée mais qui est aussi le représentant de la volonté du peuple qui doit garantir la protection effective des droits et libertés fondamentales » notamment, comme le note la Charte, par la création d'une autorité de contrôle. « Indeed, citizens trust government more than the private sector

65. F. Sudre, «Existe-t-il un ordre public européen? » in P. Tavernier, Quelle Europe pour les Droits de l'Homme, Bruxelles-Bruylant, 1996, 53.

66. A cet égard, les multiples décisions de la Cour de Justice des Communautés européennes qui ont précédé l'insertion par le Traité d'Amsterdam de cet article 6, P. Wachsman, Les droits de l'Homme, RTD européen, 1997, n° 4, p. 883-902 en particulier l'arrêt Wachauf du 13 juillet 1989, Aff. 5/88, Rec. 2609: « En vertu d'une jurisprudence constante, les droits fondamentaux font partie intégrante des principes généraux du droit dont la Cour assure le respect. En assurant la sauvegarde de ces droits, la Cour est tenue de s'inspirer des traditions constitutionnelles communes aux Etats membres, de telle sorte que ne sauraient être admises dans la Communauté des mesures incompatibles avec les droits fondamentaux reconnus par les Constitutions de ces Etats ».

67. C. Leben, « Y a-t-il une approche européenne des Droits de l'Homme? », in L'Union européenne et les Droits de l'Homme, op. cit., p. 98.

68. C. Leben fait allusion à la Déclaration des droits et devoirs de l'Homme proclamée lors de la déclaration d'indépendance des Etats-Unis, contemporaine de la déclaration de la révolution française.

with personal information...In this context, European democracies approach data protection as an element of public law. »[69].

28. Le discours américain est différent: le premier amendement consacre la liberté d'expression, il est considéré dans le secteur privé comme le fondement même de la liberté de circulation de l'information y compris nominative[70]. Ceci n'empêche pas, comme le notent nombre d'auteurs américains[71], la nécessité dans certains secteurs de protéger la personne concernée non en tant que citoyen, bénéficiant de droits fondamentaux mais en tant que consommateur individuel, devant être protégé contre les abus potentiels que le rapport inégalitaire de force permet dans certains secteurs. Cette approche « consumers' privacy » explique que dans le secteur privé, les initiatives réglementaires aux Etats-Unis n'ont visé que peu de secteurs, en particulier celui du crédit[72] mais que pour les mêmes raisons, certains[73] préconisent demain l'octroi par la législation de « privacy

69. J. Reidenberg, art. cité, Houston Law Rev., p. 731.

70. «It was also undestood that in somle circumstances yhe first Amendment presumption against government restrictions on speech would not allow certain privacy laws that limited publication of personal information by news organizations» (M. Rothenberg, Fair Information Practices and the Architecture of Privacy, 2001 Stan. Tech. L. Rev.,1, n°29)

71. P. Schwartz – J. Reidenberg, Data Privacy Law. «A Study of U.S. data Protection», Michie Law Publishers, Virginia, 1996; G.M. Connor, Privacy Policies under Gramm-Leach, New-Jersey L.Journ., 8 mai 2000; A. Bartow, Our Data, ourselves: Privacy, Propertization and Gender, 34 U.S.F. L. Rev., (2000), 633

72. Ainsi, le secteur du crédit depuis le Fair Credit Reporting Act de 1970, le Fair Credit Billing Act de 1974, l'Equal Credit Opportunity Act de 1974, Le Right to financial Privacy Act de 1978 ... dans d'autres secteurs, à noter celui des télécommunications avec l'Electronic Communications Privacy Act de 1986, le Cable Communications Policy Act de 1984, le Telephone Consumer Protection Act de 1991 et plus récemment, le Children's Online Privacy Act de 1998 et les importants « Standards for Privacy if Individually Identifiable Health Information Regulation Texts (Medical Privacy Act) », OCR HIPAA Privacy, Oct 2002, disponibles sur le site: http://www.hhs.gov/ocr/combined.regtext.

3. On rappelle que dans son rapport au Congrès sur l' Online Privacy après avoir plaidé dans ses rapports de 1998 et 1999 pour des solutions mises au point par le marché lui-même reconnaissait dans son rapport du 22 mai 2000, l'intérêt d'une législation pour protéger la vie privée des consommateurs dans le cadre des transactions via Internet (Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission report to the Congress disponible sur le site: http://www. ftc.gov/os/2000/05/index.htm#22. Pour être complet, on ajoutera que le nouveau président de la F.T.C. Mr T. Muris, se prononca contre un mouvement de légifération en ce domaine: « Remarks at the Privacy 2001 Conference, Protecting Consumers' Privacy: 2002 and Beyond», (Oct. 4, 2001), discours disponible sur le site de la FTC.

rights » en matière d'Internet où les risques d'atteinte aux intérêts des individus sont à craindre au vu des technologies utilisées pour la collecte et des larges capacités de traitement que ces technologies autorisent. Ceci dit, en admettant même cette extension importante, il n'est point question pour le législateur américain de remettre en cause le paradigme selon lequel la « privacy » est d'abord un problème de balance d'intérêts privés, vis-à-vis de laquelle l'Etat n'a point fondamentalement à intervenir sauf cas exceptionnels.

La déclaration sous l'ancienne présidence Clinton de la Maison Blanche du 1er juillet 1997 à propos du commerce électronique global[74] illustre bien les limites strictes de l'intervention de l'Etat: « *Americans treasure privacy, linking it to our concept of personal freedom and well-being* ». « *At the same time, fundamental and cherished principles like the First Amendment, which is an important hallmark of American democracy, protect the free flow of information. Commerce on the GII (Global Information Infrastructure) will thrive only if the privacy rights of individuals are balanced with the benefits associated with the free flow of information".*

"The Administration supports private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes. These include mechanisms for facilitating awareness and the existence of choice online, evaluating private sector adoption of and adherence to faire information practices, and dispute resolution".

"The Administration supports private sector efforts now underway to implement meaningful, consumer-friendly, self-regulatory privacy regimes. These include mechanisms for facilitating awareness and the existence of choice online, evaluating private sector adoption of and adherence to fair information practices, and dispute resolution".

"The Administration also anticipates that technology will offer solutions to many privacy concerns in the online environment, including the appropriate use of anonymity. If privacy concerns are not addressed by industry through self-regulation and technology, the Administration will face increasing pressure to play a more direct role in safeguarding consumer choice regarding privacy online".

"To ensure that differing privacy policies around the world do not impede the flow of data on the Internet, the United states will engage its key trading

74. «A framework for Global Electronic Commerce », The White House, 1 July 1997, Available at http://www.ecommerce.gov/framework.htm.

partners in discussions to build support for industry-developed solutions to privacy problems and for market driven mechanisms to assure customer satisfaction about private data is handled".

29. L'approche européenne fondée sur les droits de l'Homme confère à l'Etat un rôle plus proactif. Il s'agit de le consacrer non seulement à travers une solution législative non point spécifique à un secteur mais générale mais surtout d'en garantir publiquement le respect effectif à travers la création d'autorités indépendantes de contrôle et des incriminations pénales[75]. Au-delà, cette approche interdit que la balance entre les intérêts de la personne concernée et ceux du responsable du traitement, principe essentiel des privacy standards, puisse être évaluée des seuls points de vue de ces personnes mais doit faire l'objet d'une réflexion publique démocratique qui interdit toute négation même par une personne consentante de sa dignité humaine[76].

30. En aucune manière, l'information nominative ne peut être considérée exclusivement comme une simple « commodity »[77], mais renvoie à une

75. L'existence de ces « incriminations pénales » témoigne de la volonté des autorités européennes de mettre leurs services de police et la justice au service de ce droit fondamental.

76. « A property-based regime of the type Lessig describes lacks any commitment to an institutional structure (por more broadly democratic institutions) that could be established to protect an underlying public interest. Privacy interest that cannot be expressed in a marketplace through the exercise of P3P preferences simply do not exist. Again interests of common concern are pushed aside in the name of promoting market-based negotiation. Such an approach implicates not only public values but also public debates and public institutions. A regulatory regime also allows the design of an architecture that reflects public values as opposed to simply private market power.»

77. M. Rothenberg, art.cité, n° 95: l'auteur critique violemment du moins en ce qui concerne la protection des données personnelles, l'approche « libertarienne » de Lessig (Code and other Laws of Cyberspace) qui plaide pour une non intervention de l'Etat)
A ce propos, voir L. Berkamp qui plaide pour une approche de la vie privée en termes de « commodity » négociable (Lucas Berkamp, « EU Data Protection Policy. The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-driven Economy », Computer Law & Security Report Vol. 18 No 1, 2001, pp. 31-47). A propos de l'incorporation du droit à la protection des données dans la Charte européenne des Droits de l'Homme, l'auteur écrit: « An unfortunate consequence of including this right among truly fundamental rights, such as the prohibition of torture and slavery and the freedom of expression, is that the notion of fundamental right seriously devaluated, with adverse consequences for the respect for the core human rights ».

réflexion sur la liberté humaine[78] excluant toute approche fondée sur la « propriété » par la personne concernée de ses données nominatives[79].

Notre réflexion ne vise pas à interdire toute cession ou toute possibilité pour une personne consentante de pouvoir disposer de ses données nominatives. Le consentement de la personne concernée, qu'il soit simple, indubitable, expresse ou par écrit, est, dans la directive, la première cause de légitimité d'un traitement de données à caractère personnel mais ce fondement n'exclut pas marginalement l'intervention d'un juge lorsque la renonciation à l'exercice du droit à la vie privée[80] représente de par les circonstances, la nature des données concédées et/ou la puissance du responsable du traitement en question[81] une renonciation au droit et non simplement à l'exercice d'un droit[82]. En outre, le droit à la vie privée étant un droit de l'Homme, « la renonciation au bénéfice de ce droit serait d'autant plus difficilement admissible qu'une obligation positive pèserait sur l'Etat à l'effet d'assurer la jouissance effective du droit en cause »[83], c'est-à-dire de doter l'individu des moyens qui permettent l'exercice effectif de ses droits[84].

A cet égard, le rôle positif de l'Etat est multiple. Il ne s'agit pas simplement de prescrire les modalités suivant lesquelles le consentement sera réellement éclairé et spécifique et cela sous le contrôle des autorités publiques mais en outre, a posteriori, de s'interroger sur la proportionnalité de la renonciation, le juste équilibre entre l'objectif poursuivi par les ingérences consenties et les restrictions subies[85] à la libre détermination de l'individu.

On notera simplement dans le contexte de la présente contribution que l'information nominative ne peut simplement s'assimiler selon le raisonnement européen à une simple valeur économique soumise à la discrétion de celui qu'elle concerne ou de celui qui la traite. La valeur de l'information nominative doit s'apprécier en termes de relations de pouvoir entre la personne concernée et celui qui traite la donnée. Cette relation de pouvoir a un impact sur le degré d'autonomie et de liberté des individus et impli-

78. A ce propos, P. Schwartz, Privacy and Democracy in Cyberspace, 52 Vanderbilt Law Rev. 1609, 1661, 1999 et plus récemment, D.J. Solove, Conceptualizing Privacy, 90 California Law Rev., 1087 (1115), 2002. " Schwartz also questions the assumption that individuals are able to exercise meaningful choices, with regard to their information, given disparities in knowledge and power when bargaining over the transfer of their information. The implication is that privacy involves not only individual control, but also the social regulation of information. In other words, privacy is an aspect of social structure, an architecture of information regulation, not just a matter for the exercise of individual control.". On notera que cette réflexion en termes d'équilibre des pouvoirs entre les personnes concernées et les responsables de traitement et la nécessité d'une intervention de l'Etat, est omniprésente aux Etats-Unis lorsqu'il s'agit de traitements opérés par les autorités publiques et on comprend mal pourquoi ce même raisonnement n'est pas adopté lorsqu'il s'agit de traitements opérés dans le secteur privé.

79. Sur cette distinction fondamentale des approches, Y. Poullet, «Data Protection between Property and Liberties: a civil Law approach», in Amongst Friends in Computer and Law, R. Kaspersen and A. Oskamp (ed.), 1990, p. 175 et ss.; J. E. Cohen, «Cyberspace and Privacy: A new legal Paradigm», 52 Stanford L. Rev. 2000, 1373 et ss.: «Things deemed property are not defined solely or even primarily by their exchange value but rather by the ways by which they shape the social relations between and among persons... Equating "privacy" with "property" disfavors strong data privacy protection only to the extent that our sense of what can be owned is limited by a platonic ideal of frictionless tradability. Other insights point the way toward a more nuanced understanding of the social and institutional roles of things deemed property....»

80. Sur cette distinction et l'admission de la renonciation à l'exercice d'un droit fondamental mais non à un droit, lire Ph. Frumer, «La renonciation aux droits et libertés, Coll. Droit international, Bruylant, Bruxelles, Ed. ULB, 2001, en particulier, p. 340 et la nombreuse doctrine y citée, en particulier Fr. Rigaux.

81. En particulier, il y a lieu de craindre que des systèmes comme le P3P ne généralise la pratique des transactions économiques: la personne concernée se voyant proposer des réductions substantielles de prix contre la transmission de données personnelles ou l'utilisation de ses données personnelles à des fins marketing quelconques, cette pratique créant une discrimination en défaveur de ceux qui ne pourront se payer le luxe de la protection de leur vie privée.

82. Cf. déjà W.G. Ganshof Van Der Meersch, «La Convention européenne des droits de l'homme a-t-elle, dans le cadre du droit interne, une valeur d'ordre public? » in Les droits de l'Homme en droit interne et international, Bruxelles, Presses Universitaires, 1968, p.239.

83. Ph. Frumer, op. cit., p. 626 et sa référence au constitutionnaliste américain, L. Tribe à propos des droits que cet auteur qualifie de « systématiques » c'est-à-dire « liés à des relations structurelles de pouvoir et dont la raison d'être est d'empêcher la perpétuation d'une domination de certains individus sur d'autres ... » (définition particulièrement appropriée à propos des relations entre les individus et certaines entreprises disposant de larges ressources informationnelles ».

84. « Finally, effective data privacy legislations also must incorporate other non consent-based requirements for fair information practices. The notion that informed consent alone is sufficient to protect individual interests in the uses of personally identified data is peculiarly American one. Internationally agreed principles of fair information practices require a variety of other substantive and procedural protections....These principles are designed to ensure that data processors are held accountable to individuals... Accountability has collective as well as individual dimensions...» J.E. Cohen, «Cyberspace and Privacy: a new legal Paradigm», 52 Stanford L. Rev., 2000, p.1373 et ss.

85. On notera à cet égard que le consentement n'est qu'un facteur d'appréciation certes important mais non décisif de cet examen de proportionnalité.

que le devoir de l'Etat de définir les conditions de légitimité minimale de cette relation de pouvoir afin de protéger la dignité des personnes[86].

B. Ce droit fondamental fait partie d'un « ordre public communautaire »

31. L'obligation des Etats européens et de l'Union européenne de veiller au respect des droits fondamentaux consacrés par la Convention européenne, en particulier de la vie privée a, nous l'avons souligné, un caractère objectif: « Les obligations souscrites par les Etats contractants dans la Convention ont essentiellement un caractère objectif, du fait qu'elles visent à protéger les droits fondamentaux des particuliers contre les empiétements des Etats contractants, plutôt qu'à créer des droits subjectifs et réciproques entre ces derniers » affirmait, dès 1961, la Commission européenne des Droits de l'Homme[87].

L'arrêt Irlande contre Royaume Uni[88] distingue à cet égard, la convention européenne des droits de l'Homme des autres Traités internationaux[89]. « En sus d'un réseau d'engagements synallagmatiques bilatéraux (la Convention) crée des obligations objectives qui, aux termes de son préambule, bénéficie d'une « garantie collective » ... La Convention ne se contente pas d'astreindre les autorités suprêmes des Etats contractants à respecter elles-mêmes les droits et libertés qu'elle consacre; .... Elle implique aussi qu'il leur faut, pour èn assurer la jouissance, en empêcher ou corriger la violation aux niveaux inférieurs ».

86. Sur ce point, nous ne pouvons que renvoyer le lecteur au remarquable article de J.E. Cohen, « Cyberspace and Privacy: a new legal Paradigm? », 52 Stanford L. Rev., 2000: « First informational Autonomy comports with important values concerning the fair and just treatment of individuals within society. From Kant to Rawls, a central strand of Western philosophical tradition emphazises respect for the fundamental dignity of the persons and a concomitant to egalitarianism in both principle and practice. ...(This approach) requires that we forbid data processing practices that treat individuals as mere conglomerations of transactional data;, or that rank people as prospective consumers, employees or insured based on their financial or genetic desirability. The drafters of the directive agreed with this characterization: the directive is explicitly grounded in the fundamental rights and freedom of natural persons».

87. Comm. Eur.d. h., 11 janv. 1961, reg. N° 788/60, Autriche c. Italie, Ann. CDH, 1961, p. 141.

88. Arrêt Irlande c. Royaume-Uni, 18 janv. 1978, Rec. des arrêts de la Cour, Série A, n° 25, § 239.

89. A propos de cette distinction, l'étude proposée par L.A. Bygraeve, «Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, 6, Int. Journal of Law and Information Technology, 2000, n°3, p.247 et s.: l'auteur étudie la signification du Right to Privacy selon l'article 17 du pacte international des droits civils et politiques et selon l'article 8 de la Convention européenne des droits de l'Homme.

Comme l'écrit Yernault[90], « l'ensemble qui réunit ces obligations objectives et le système de garantie collective qui les protège font de la Convention, « l'instrument constitutionnel[91] de l'ordre public européen », selon l'expression forte consacrée dans l'arrêt sur les exceptions préliminaires dans l'affaire Loizidou[92] ».

L'arrêt Loizidou est salué par nombre de commentateurs[93] comme la reconnaissance claire du statut de la Convention et des droits de l'homme y consacrés comme éléments de l'ordre public européen, au sein des Etats membres de la Convention et, de ce fait, des Etats membres signataires du traité de l'Union européenne.

32. Cette approche des « droits de l'Homme » comme élément constitutif de l'ordre public européen est affirmée plus clairement encore par le traité de l'Union européenne. L'article 6 § 1 du Traité de l'Union européenne introduit par le Traité d'Amsterdam, en affirmant que « L'Union est fondée sur les principes de la liberté, de la démocratie, du respect des droits de l'Homme et des libertés fondamentales, ainsi que de l'état de droit, principes qui sont communs aux Etats membres » souligne en effet l'existence d'un certain nombre de principes participant au patrimoine commun de la société européenne. « L'idée essentielle est bien de sortir les

90. D. Yernault, «De la fiction à la réalité: le programme d'espionnage électronique global», « Echelon et la responsabilité internationale des Etats au regard de la Convention européenne des droits de l'homme», Rev. Belge de droit int., 2000, 1, p. 222.

91. A propos de l'article F § 2 du Traité d'Amsterdam qui a introduit l'article 6 du Traité de Rome, H. Labayle («Droits fondamentaux et droit européen, AJDA, Les droits fondamentaux, n° spécial, juillet 1998, p. 83) parle « d' opération de constitutionnalisation de l'existant ». Pour une approche critique de la notion de droit constitutionnel européen à propos de la Charte des droits fondamentaux, lire H. Dumont et S. van Droogenboeck, «La contribution de la Charte à la constitutionnalisation du droit de l'Union européenne, in La charte des droits fondamentaux de l'Union européenne, Ouvrage collectif, Bruxelles, Bruylant, 2002.

92. Arrêt Loizidou c. Turquie, 23 mars 1995, Rec. des arrêts, Série A, n° 310, § 75. En ce sens les réflexions de G. Cohen-Jonathan et J.-F. Flauss, « De l'office de la Commission européenne des droits de l'homme dans la protection des droits fondamentaux de l'Union européenne: L'arrêt Matthews», Rev. Droits de l'Homme, 1999, 253.

93. Cf. not. F. Sudre, Existe-t-il un ordre public européen? In P. Tavernier, Quelle Europe pour les droits de l'homme? Bruxelles, Bruylant, 1996, p. 39; J.-F. Flauss, « Les droits de l'homme comme élément d'une constitution et de l'ordre européen», Les Petites Affiches, n° 52, 1993, p. 10; G. Karydis, L'ordre public dans l'ordre juridique communautaire: un concept à contenu variable, RTD eur. 2002, 1, p. 1 et s; J. Andriantsimbazoniva, « L'élaboration progressive d'un ordre public européen des droits de l'Homme», Cah. Dr. Europ., 1997, n° 5/6, p. 655.

libertés individuelles du domaine réservé des Etats pour en faire l'objet d'un ordre public européen ... »[94].

« La notion d'ordre public[95] cherche à traduire « les exigences fondamentales d'une vie en société ». En ce sens, la Convention européenne des droits de l'homme est un instrument constitutionnel de l'ordre public européen. Elle tend à assurer au nom des valeurs communes et supérieures aux Etats parties, la protection des individus qui vivent sous l'autorité nationale »[96]. Le caractère impératif de la règle d'ordre public s'impose tant en interne qu'en externe. « Ces effets se déploient d'abord au sein du cercle des seuls Etats contractants – ce sont là les contraintes « internes » de l'ordre public européen – mais ils débordent aussi ce cadre et intéressent les Etats tiers empruntant le mécanisme de l'exception d'ordre public »[97]. C'est ce dernier point qui, selon nous, fonde et justifie les articles 25 et 26 de la directive européenne mais au-delà l'action énergique de l'Union européenne sur le plan international en faveur du respect de la vie privée. Nous reviendrons sur cette affirmation plus loin.

94. J.F. Renucci, « Droit européen des Droits de l'Homme», 2ème éd., LGDJ, 2001, p. 429; F. Ost, Originalité des méthodes d'interprétation de la Cour européenne des droits de l'Homme, in M. Delmas-Marty, Raisonner la raison d'Etat, PUF, 1989, p. 458.

95. Sur les relations entre ordre public et droits fondamentaux, lire l'excellent ouvrage collectif publié sous la direction de M.J. Redor, L'ordre public, ordre public et droits fondamentaux, publié dans la collection « Droit et Justice », Bruylant, 2001.

96. F. Sudre, Existe-t-il un ordre public européen?, in P. Tavernier, « Quelle Europe pour les droits de l'homme? », op. cit., p. 39 et s.

97. F. Sudre, art. cité, p. 59.

33. En effet, "selon la jurisprudence de la Cour de Justice des Communautés Européennes, le droit au respect de la vie privée (...) constitue l'un des droits fondamentaux protégés par le droit communautaire[98] »[99] qui, ajoutent le Conseil et la Commission, « mérite une attention particulière dans notre société de l'information, qui évolue rapidement »[100].

Récemment, la Charte des droits fondamentaux de l'Union européenne[101] consacre explicitement en ses articles 7 et 8 ce droit fondamental[102]. L'analyse du texte des deux articles mérite une attention particulière. Alors que l'article 7 évoque le droit de chacun au respect de sa vie privée, de son

98. Nombre de constitutions européennes reconnaissent le droit à la vie privée comme un droit constitutionnel, ainsi, la Constitution portugaise (article 35), la Constitution espagnole (article 18), la Constitution belge (article 21), la Constitution des Pays-bas (article 10), etc.. On sait qu'en Allemagne, la Cour constitutionnelle a déduit directement de l'article 3 consacrant le droit à la dignité et à l'autodétermination, le principe de la protection des données.

99. C.J.C.E., 5 octobre 1994 x c. Commission, aff. C 404/92 P. Rec., I 4737, point 17. cf. déjà C.J.C.E. 18 mai 1989, Commission c. RFA, aff. 249/86, Rec. 1263, point 10: Le respect de la vie familiale « fait partie des droits fondamentaux, qui, selon la jurisprudence constante de la cour, sont reconnus par le droit communautaire ». Sur les nombreux jugements (38 arrêts de la Cour et 19 jugements du Tribunal de 1ère Instance jusqu'en octobre 1999) qui se réfèrent à la vie privée, lire J. Andriantsimbazoniva, Le droit au respect de la vie privée et familiale, in Réalités et perspectives du droit communautaire des droits fondamentaux, F. Sudre et H. Labayle (éd.), Coll. Droit et Justice, Bruxelles, Bruylant, 2000, p. 253 et s.

100. Plan d'action du Conseil et de la Commission concernant les modalités optimales de mise en œuvre des dispositions du Traité d'Amsterdam relatives à l'établissement d'un espace de liberté de sécurité et de justice, Texte adopté par le Conseil Justice & Affaires intérieures, le 3 déc. 1998, JOCE, n° C.19 23 janvier 1999.

101. ... adoptée conjointement par les 3 institutions communautaires, le 7 décembre 2000 (JOCE C 364/2000, p. 1) disponible sur le site: http://europa.eu.int/comm/justice_home/unit/charte/pdf/texte_fr.pdf. Sur la valeur de cette charte, lire la Communication de la Commission sur la nature de la Charte des droits fondamentaux de l'Union européenne, Bruxelles 11 oct. 2000, Com (2000) 644 final, point 10. En outre, « Finalement, la Charte des droits fondamentaux, telle qu'adoptée lors du Sommet de Nice, n'a pas d'effet contraignant; il faut néanmoins s'attendre à ce qu'elle exerce une certaine influence sur la pratique juridique », Hans C. Kruger et Jörg Polakiewicz, « Propositions pour la création d'un système cohérent de protection des droits de l'homme en Europe » Revue Universelle des Droits de l'Homme, vol. 13, n° 1-4 2001.pp. 1-14. De manière plus positive, « Elle est donc déjà plus qu'une promesse: un instrument juridique dont l'effectivité dépendra de l'utilisation que les plaideurs en feront. » H. Bribosia et O. de Schutter, « La Charte des droits fondamentaux de l'Union européenne», J.T., 2001 , p. 282. Sur cette charte, lire le n° spécial consacré par la même Revue universelle des Droits de l'Homme, Vol. 12, n° 1-2, 2000, p. 1-84: « La Charte des droits fondamentaux de l'Union européenne», Actes des Journées d'études sous la direction de Fl. Benoit-Rohmer, Strasbourg, 16-17 juin 2000.

domicile et de sa correspondance, l'article 8 évoque distinctement le droit à la protection des données. Il énonce ce droit comme suit:

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant; 2. Ces données doivent être traitées loyalement à des fins déterminées et sur base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification; 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

34. On note que la Charte élargit ainsi considérablement la portée de l'article 8 de la Convention européenne des Droits de l'Homme dont pourtant elle s'inspire.

- Premièrement, la Charte ne se contente pas d'une protection contre les seules autorités publiques mais étend cette protection à l'ensemble des traitements y compris dans le secteur privé au moment même où l'effet dit « horizontal » de la Convention[103] est toujours discuté et surtout au moment où la Cour de Strasbourg n'a jamais connu de décisions qu'à propos de l'autorité publique[104]. Il est donc clair que l'Union européenne souhaite un élargissement du droit fondamental à la protection des données personnelles à l'ensemble du secteur privé.
- Deuxièmement, la Charte affirme clairement que la protection des données ne se limite pas à la protection de l'intimité ou de la confidentialité, conception négative et traditionnelle de la notion de vie privée mais que de manière positive, elle s'élargit à la protection de la personnalité contre les atteintes de toute forme de pouvoir qu'il soit privé ou public et s'apparente alors au droit à l'autodétermination,[105] exigeant une certaine transparence des traitements et le respect d'une balance entre les intérêts légitimes des responsables des traitements et ceux des personnes concernées[106]. Ce clair élargissement de la vie privée à la protection des données conduira sans doute la jurisprudence de la Cour luxembourgeoise à se montrer plus hardie que la Cour strasbourgeoise dans la défense de ce droit fondamental[107].

Enfin, selon la Charte, un des éléments essentiels de la protection du droit fondamental ainsi reconnu est la création et l'action d'une autorité publique indépendante de protection des données[108], capable d'assurer aux citoyens l'effectivité de leur droit fondamental.

C L'obligation de l'Union européenne de veiller au respect des droits de l'homme et à la protection des données relatives à ses citoyens dans les relations internationales

35. Il s'agit bien d'affirmer haut et clair la souveraineté européenne, conçue non plus comme la défense d'un territoire physiquement délimité par des frontières mais, dans un ordre global, comme une obligation mise à charge de l'Etat de garantir dans le cyberespace le respect des libertés indi-

102. On lira sur la nécessité de reconnaissance, la Recommandation 4/99 du Groupe de travail de l'article 29, en date du 7 septembre 1999, à propos de l'inclusion du droit fondamental à la protection des données dans le catalogue européen des droits fondamentaux (recommandation sur le site de la Commission à l'adresse suivante: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp26en.htm ».

103. A propos de l'effet horizontal de l'article 8 de la Convention européenne des droits de l'Homme, parmi d'autres lire D. Spielmann, « L'effet potentiel de la Convention européenne des droits de l'Homme entre personnes privées», Bruxelles, Bruylant - Nemesis, 1995.

104. Comme le note in fine L. Bygraeve: « However, an important challenge for the European Court of Human Rights in the future will be the data processing practices of private sector entities: how the Court tackles these practices will determine to a large extent the long-term utility of Art 8 as an instrument for Data protection » (L. Bygraeve, Data Protection pursuant to the Right to privacy in Human Right Treaties, Int. Journal of Law and Inf. Technology, 6, n°3, p.284; dans le même ordre d'idées, O de Schutter, «Vie privée et protection de l'individu», note sous l'arrêt Rotaru, CEDH 4 mai 2000, Rev. Trim. Droits de l'Homme, 2001, p. 149 et ss.

105. A ce propos, lire P. De Hert, Het Europees Hof van Rechten erkent publieke privacy, N.J.W., 2002-03, 116-122: l'auteur insiste sur la « constitutionnalisation » (constitutionaliesering) européenne du droit à la protection des données au delà du droit traditionnel à la « vie privée », opérée par la Charte européenne des droits de l'Homme.

106. Sur cette distinction de ces deux conceptions de la vie privée et d'autres gravitant autour de ces deux pôles, lire D.J. Solove, Conceptualizing Privacy, 90 Cal. Law Review, 2002, 1087-1155. L'auteur montre que toute définition de la vie privée est vaine et que cette notion ne peut être approchée qu' à partir de diverses acceptions, entre lesquelles la notion oscille suivant les circonstances: « Trying to solve all privacy problems with a uniform and overarching conception of privacy is akin to using a hammer to insert a nail into the wall but also to drill a hole » (p. 1147) et à propos de la réduction fréquente du débat à la seule protection de la confidentialité: « Secrecy as the common denominator of privacy makes the conception of privacy too narrow. » (p.1109)

107. A propos de cette concurrence entre les deux institutions dans le domaine de la reconnaissance du droit à la vie privée, lire les réflexions de O. de Schutter, art.cité.

108. Par là, la Charte ne fait que renforcer l'importance des «autorités de contrôle » dont la directive 95/46 consacre les compétences en son article 28.

viduelles de ses citoyens[109]. L'appartenance d'un individu à un Etat lui donne le droit de bénéficier d'une protection par cet Etat des garanties et libertés constitutionnelles qui lui sont reconnues. Ces garanties et libertés ne peuvent être remises en cause du seul fait que les technologies de l'information et de la communication ignorent désormais les frontières physiques[110]. En d'autres termes, la souveraineté étatique apparaît comme « une manifestation d'indépendance »...La souveraineté n'est point en soi un point d'aboutissement; elle est le « moyen, pour les pouvoirs établis de pourvoir aux besoins des nationaux et d'assurer à ceux-ci et aux étrangers vivant sur son territoire le libre exercice de leurs droits »[111]. Notre dernier point est consacré aux conséquences de cette affirmation en matière de protection des données.

36. L obligation, mise à charge des Etats, obligation de vigilance ou de diligence due en matière de respect des droits de l'Homme dans le cadre des relations internationales qui peuvent se nouer entre les ressortissants de l'Union européenne et de pays-tiers, a été historiquement développée dans le cadre de la protection due aux ressortissants étrangers sur le territoire d'un état tiers (protection des diplomates). Dans le cadre d'une société de plus en plus caractérisée par les échanges internationaux, l'article 13 de la Convention européenne des droits de l'Homme[112], qui consacre le droit des citoyens de l'Europe a un recours effectif devant une instance

09. Sur ce point, lire les développements de Y. Poullet et J-M. Dinant, « Le réseau Echelon: Existe-t-il? Que peut-il faire? Peut-on et doit-on s'en protéger» , Rapport d'expertise rédigé à l'attention du Comité de surveillance des services de renseignements, 7 mars 2000 publié in extenso in Comité permanent de contrôle des services de renseignements, Rapport complémentaire d'activités, 1999, pp. 13 et s.

10. A ce propos, lire J. Barberis, « Les liens juridiques entre l'Etat et son territoire: perspectives théoriques et évolution du droit international», Annuaire français de droit international, 1999, p. 132 et ss.

11. R. Wilkin, V° Souveraineté, Dictionnaire de droit public, Bruxelles, Bruylant, 1963. Sur cette notion moderne de souveraineté et son lien avec le territoire, lire F. Hamon et M. Troper, Droit constitutionnel, Manuel, 21ème éd., LGDJ, Paris, p.21: « ... on peut dire qu'il n'y a pas d'Etat sans territoire. Non pas que le territoire soit, comme on le croit parfois, un élément constitutif de l'Etat; mais parce qu'il est une condition indispensable pour que l'autorité politique s'excerce efficacement. »

12. J.F. Flauss, « Le droit à un recours effectif. L'article 13 de la Convention européenne des droits de l'Homme », Rev. Univ. Droits de l'Homme, 1991, p.324; G.H. Tunc, «The Right to an effective Remedy in domestic Law», in Broadening the frontiers of Human rights, Scandinavian Univ. Press, 1992, p. 78 et ss..

nationale pour contester les violations de la Convention, a également été invoqué. Bref, comme le note Yernault[113], l'article 13 de la Convention, comme les obligations positives inhérentes à la protection des autres droits garantis, a pour conséquence que les Etats ont le devoir de prévenir les violations quels qu'en soient les auteurs (organes de l'Etat, personnes privées, personnes internationales tierces) et en cas de violations d'enquêter, de punir celles-ci ainsi que, le cas échéant, de les réparer ». Pour justifier cette obligation de vigilance, l'auteur cité se réfère en outre à une décision de la Cour interaméricaine des droits de l'Homme de 1988: « Il est clair qu'est imputable à l'Etat toute violation des droits reconnus par la Convention (interaméricaine des droits de l'Homme) résultant d'un acte des pouvoirs qu'ils tirent de leurs fonctions officielles. Cela n'épuise cependant pas les situations où un Etat est obligé de prévenir, rechercher et sanctionner les violations des droits de l'Homme, ni les cas où sa responsabilité peut se voir engagée pour atteinte à ces mêmes droits. En effet, un acte attentatoire aux droits de l'Homme et qui initialement, ne serait pas directement imputable à un Etat- par exemple, s'il est l'œuvre d'un particulier ou si son auteur n'est pas identifié- peut néanmoins engager la responsabilité de l'Etat, non en raison du fait lui-même, mais en raison du manque de diligence pour prévenir la violation des droits de l'Homme ou la traiter dans les termes requis par la Convention ».

37. Comment ne pas voir dans cette jurisprudence et dans cette doctrine tirées de la Convention européenne des droits de l'Homme, la claire justification des articles 25 et 26 de la Directive. La reconnaissance de la protection des données comme un droit fondamental du citoyen européen oblige le législateur européen à prévenir les risques d'atteinte à ce droit, risques liés à la dimension internationale des réseaux et à la multiplication des flux transfrontières. Sur ce point, on ajoutera le principe de précaution[114] qui clairement reconnu par la législation européenne en matière

113. D. Yernault, L'efficacité de la Convention européenne des droits de l'Homme pour contester le système " Echelon3, in Commission mixte Chambre- Sénat du suivi du Comité « R »26 juin 2001, Annales Parl. Sénat, session 2002-/54/2 – 2001/2002 (Doc 50 1660/002 annexe 6).

114. Selon l' Union européenne, le principe de précaution a la valeur d'une règle coutumière générale de droit international. Sur ce point, les Etats-Unis ne partagent pas ce point de vue et ne voient dans ce principe rien de plus qu'une « approche » des problèmes et non une règle. Cf. à ce propos, les remarques du rapport Kowilsky-Viney remis au premier Ministre français le 15 octobre 1999 dans le cadre des négociations OMC (La documentation française, 1999, p. 115 et ss.)

d'environnement[115], devrait pouvoir également s'appliquer dans le domaine de la défense des libertés, de la vie privée en particulier: « *Le principe de précaution définit l'attitude que doit observer une personne qui prend une décision concernant une activité dont on peut raisonnablement supposer qu'elle comporte un danger grave pour la santé et la sécurité des générations actuelles ou futures ou pour l'environnement. Il s'impose spécialement aux pouvoirs publics qui doivent faire prévaloir les impératifs de sécurité sur la liberté des échanges entre particuliers et entre Etats. Il commande de prendre toutes les dispositions permettant, pour un coût économiquement et socialement supportable, de détecter et d 'évaluer le risque, de le réduire à un niveau acceptable et si possible de l'éliminer, d'en informer les personnes concernées et de recueillir leurs suggestions sur les mesures envisagées pour le traiter. Ce dispositif de précaution doit être proportionné à l'ampleur du risque et peut être à tout moment révisé.* » [116].

38. Le concept de « développement durable »[117], inscrit à l'article 2 du traité de l'Union européenne est également évoqué pour justifier les dispositions en matière de protection des données. Ce concept élargit la notion de « dommage », notion qui traditionnellement se limite aux seuls

Le lecteur se référera sur ce point aux développements de N. de Saedeleer, Les principes du pollueur-payeur, de prévention et de précaution, Thèse, Bruylant, 1999.

Rapport Kowilsky-Viney, op.cit.

Sur cette notion, lire X. Thunis, « Le développement durable, une seconde nature », Aménagement-Environnement, 2000, n° spécial, p. 9 et ss. et les nombreuses références y citées. L'auteur conclut: « Le développement durable, en se précisant, pourrait constituer ce début de vision commune en même temps qu'une exigence inspiratrice de la pratique politique et institutionnelle. Il y faudra du souffle et de la patience. Peut-on mieux faire pour s'en donner, que de lire l'avertissement prophétique de Bergson: '...qu'on opte pour les grands moyens ou pour les petits, une décision s'impose. L'humanité gémit, à demi écrasée sous le poids des progrès qu'elle a faits. Elle ne sait pas assez que son avenir dépend d'elle. A elle de voir d'abord si elle veut continuer à vivre. A elle de se demander ensuite si elle veut vivre seulement, ou fournir en outre l'effort nécessaire pour que s'accomplisse, jusque sur notre planète réfractaire, la fonction essentielle de l'univers, qui est une machine à faire des dieux'. »

dommages qui peuvent être déterminés de manière immédiate[118], et situe les développements technologiques dans une perspective à moyen voire à long terme en cherchant à prendre en considération leurs impacts sur les générations futures. Il convient dès lors d'anticiper les conséquences dangereuses économiques, sociales et culturelles que peut avoir ce développement. Appliqué aux technologies de la société de l'information[119], le concept de développement durable exige que le citoyen garde une maîtrise de son image informationnelle et puisse avoir accès aux bénéfices des services nés de ce développement technologique. Dans ce contexte, les législations « vie privée » et en particulier les dispositions relatives aux flux transfrontières prennent tout leur sens et trouvent leur justification. Il ne s'agit pas de lutter contre des « harmful misuses « actuellement subis par les citoyens européens mais de donner à ceux-ci contre les risques de développement d'une société informationnelle de contrôle et liberticide, certaines garanties minimales de protection de leurs libertés et de leur dignité[120].

39. L' atteinte à la protection des données peut être perpétrée alors même que la personne ne quitte pas le territoire européen mais simplement du fait que des données relatives à cette personne et donc des risques d'atteinAcet égard, on ne peut suivre le raisonnement de L. Bergkamp (E.U Data Protection Policy – The Privacy fallacy: adverse Effects of Europe's Data Protection Policy in an Information-driven Economy, 18 Computer Law and Security Report, 1,2002, 31 et ss.) qui reproche précisément à la directive de ne pas s'en tenir à la conception traditionnelle du dommage, c'est-à-dire à la seule répression des abus de traitement des données: « The EU regime regulates at the wrong level and fails to balance competing interests properly. It regulates collection and processing of data upstream, while it should regulate specific harmful uses downstream. ». Cf. également dans ce sens, R. Litan, «Balancing costs and benefits of new Privacy Mandates, AEI-Brookings Joint Research Center for Regulatory Studies, Working Paper, 99-3, April 99».

Cf. à ce propos, la conférence organisée en février 2000 par la Commission européenne à Helsinki: « Towards a Sustainable Information Society ».

" Data Protection is essential to realize the goals of a sustainable Information Society. Data Protection laws provide for mechanisms to avoid that information is processed and used outside the control or against individuals. Transparency requirements must guaranteee that data subjects remain the true subjects of their data; they should not become objects. Data protection laws present data subjects to be the victims tomorrow of unlimited data collection and processing today." (J. Dhont et M.V. Perez, « Regulating Data Protection in a Cross-Cultural Perspective», Paper rédigé dans le cadre du projet Fonds special de Recherche « Privacy: Human Liberty or Consumer Right? The US-EU Dialogue », FUNDP / CRID (étude à paraître).

te à sa vie privée sont encourus du fait de leur circulation au delà des frontières européennes.

Cette circulation peut naître d'une transmission volontaire par un responsable ou par la personne concernée de ses données vers un destinataire situé hors Europe. Dans ce contexte, les articles 25 et 26 de la Directive se conçoivent comme le complément indispensable des autres dispositions qui visent les traitements opérés uniquement sur le territoire des Etats membres. La sauvegarde des libertés ne pourrait se concevoir s'il suffisait de transférer à l'étranger les données initialement protégées pour que l'individu perde les garanties qui lui étaient accordées. Le fait que la protection des données constitue un droit fondamental implique que les Etats membres prennent des précautions pour que ce droit ne soit point violé du fait de ce transfert. En outre, l'effectivité des droits reconnus dans un système juridique donné se mesure, comme l'affirme l'article 13 de la Convention déjà cité[121], à l'étendue des garanties juridictionnelles[122]. On comprend dès lors l'importance prise dans la négociation des « Safe Harbor Principles » du rôle susceptible d'être joué par la Federal Trade Commission dans la résolution des litiges. De même dans le contrat modèle, on insiste sur la possibilité en toute hypothèse pour la personne concernée de pouvoir saisir la juridiction compétente de son Etat. L'article 4 c) instaure une règle de droit privé matériel lorsque la situation à la base du flux transfrontières présente des indices clairs de rattachement avec le pays européen d'origine de la donnée dans la mesure où le responsable du traitement fait « usage » de l' équipement sis sur le territoire de cet Etat membre sans que le transfert n'ait été initié par la personne concernée[123]. Par ailleurs, il prévient, selon un principe général de droit international, les hypothèses de contournement intentionnel d'une réglementation.

121. Cf. également sur ce point, l'article 47 de la Charte européenne des droits de l'Homme.

122. « L'effectivité du recours s'apprécie *in concreto*. Il doit être accessible à l'intéressé lui-même et adéquat de façon à permettre de dénoncer la violation alléguée. Cette effectivité du droit d'accès suppose la possibilité concrète pour un individu de contester un ingérence dans ses droits. » (J.F. Renucci, « Droit européen des droits de l'Homme », op. cit., p. 185).

123. F. Rigaux, La loi applicable à la protection des individus à l'égard du traitement automatisé des données à caractère personnel, Revue critique de droit international privé, Paris 1980, p. 443-478: « La catégorie des « lois de police » est précisément celles qui conduisent à déterminer le domaine territorial de la loi plutôt qu'à rechercher la loi applicable à une situation typique. ».

40. La circulation peut naître aussi du simple fait que les données non destinées à une personne située hors Europe circulent au hasard des réseaux sur le territoire d'autres Etats ou peuvent être captées par des autorités privées ou publiques de pays tiers. Cette hypothèse est celle révélée par les pratiques du réseau Echelon. Il s'agissait en l'hypothèse d'écoutes, par les agences de renseignements de certains pays (Etats-Unis, Royaume Uni, Nouvelle Zélande et Australie), de messages transitant par les satellites de télécommunication[124]. Ces écoutes sont opérées à partir de stations situées sur le territoire européen mais également, à partir de stations hors Europe. Dans cette seconde hypothèse où le flux n'est pas à destination d'un pays tiers, les articles 25 et 26 de la Directive sont inapplicables et comment justifier alors l'intervention européenne en faveur du respect des libertés individuelles?

Au-delà de la justification que la claire reconnaissance de la protection des données comme droit fondamental apporte aux articles de la directive relatifs aux flux transfrontières, cette reconnaissance légitime, nous semble-t-il, l'attitude de l'Europe dans les relations internationales en faveur de la reconnaissance par les Etats tiers de ce droit fondamental. L'arrêt Matthews c. Royaume-Uni rappelle que « lorsque des Etats (parties à la convention européenne) créent des organisations internationales (...) qu'ils transfèrent des compétences à ces organisations et leur accordent des immunités, la protection des droits fondamentaux peut s'en trouver affectée. Toutefois, il serait contraire au but et à l'objet de la convention que les Etats contractants soient aussi exonérés de toute responsabilité au regard de la Convention, dans le domaine d'activité concernée ». Il est piquant de constater que cet arrêt de la Cour de Strasbourg concerne précisément l'Union européenne mais il va de soi que le même principe s'applique à l'ensemble des relations internationales des pays membres de la Convention européenne[125].

124. Sur Echelon, le site de la Federation of American Scientists, http://www.fas.org/irp/program/process/echelon.htm.
A la base de la révélation des pratiques d'Echelon, le rapport de D. Campbell devant la STOA, organe consultatif du Parlement européen et depuis objet de plusieurs publications. Cf. à cet égard, l'ouvrage: Surveillance électronique planétaire, Ed. Allia, 2000 et le rapport Interception Capabilities 2000, disponible sur le site http://watserv1.uwatrerloo.ca/brobinso/cseukusa.html

125. G. Cohen-Jonathan, « Les rapports entre la Convention européenne des droits de l'homme et les autres traits conclus par les Etats parties », Mélanges Schermers, Nijhoff, 1994, T. III, p. 103-108.

La Convention du Conseil de l'Europe a, de par l'article 53 de la Convention de Vienne du 23 mai 1960 sur le droit des Traités[126], primauté sur l'ensemble des autres engagements internationaux s'ils s'avèrent moins protecteurs des droits et libertés qu'elle garantit[127]. Au niveau des Etats membres de l'Union européenne, cette attitude exigeant le respect des droits de l'homme dans les relations extérieures qu'elle noue ou que les Etats membres pourraient conclure se justifie en outre directement par

126. Selon cet article, aucun engagement international d'un Etat membre du Conseil de l'Europe ne saurait s'avérer contraire aux normes reconnues de *ius cogens*, ce que constituerait la Convention européenne des droits de l'homme.
Un autre argument pourrait être tiré de l'article 60 de la Convention européenne elle-même qui impliquerait un engagement des Etats signataires de ne pas adopter d'actes ou traités internationaux qui aient pour effet de revenir en deça de la protection accordée par la Convention elle-même (J.H.H. Weiler, Fundamental rights and territorial boundaries: on standards and values in the protection of Human rights, in N.A. Neuwalh and J. Rosas, The European union and Human Rights, Dordrecht, Martinus Nijhoff Publishers, 1995, 51-75. De manière plus prudente, lire B. Docquir, Le droit international privé à l'épreuve de la Convention européenne des droits de l'Homme, Annales de la fac. De droit de Louvain, 1999, 4,p.499 qui conclut cependant à une responsabilité des Etats signataires au cas où un Etat participerait à une convention internationale ne respectant pas les droits établis par la Convention européenne des droits de l'homme).

127. A ce propos, B. Docquir, art.cité, p.513. L'auteur au terme d'un long raisonnement conclut: « En définitive, il paraît clair que la Convention, et l'interprétation qu'en donne la Cour, jouent au moins un rôle dans la définition de l'ordre public: elles érigent le socle minimum de certains aspects de l'ordre public et empêchent un dangereux retour en arrière. On peut en effet considérer qu'une jurisprudence nationale refusant de faire jouer l'exception d'ordre public dans le sens voulu par la Convention, engagerait la responsabilité de l'Etat devant la Cour de Strasbourg. En ce sens, les droits et libertés y énoncés sont une norme supérieure à l'exception d'ordre public ».

l'article 6 du traité de l'Union européenne. Elle s'inscrit dans des nombreux textes et justifient de nombreuses initiatives[128].
Une telle affirmation s'impose à propos de la participation de l'Union européenne et des autres Etats européens à l'OMC, dont les règlements ne peuvent en aucune manière affaiblir la protection des données que la convention et la directive entendent reconnaître aux citoyens européens[129].

Elle est à la base de la condamnation extrêmement nette prononcée par le Parlement européen à propos du réseau Echelon et des Etats dont le Royaume-Uni ayant souscrit aux accords internationaux dits UKUSA ayant présidé à la création et organisant le fonctionnement du réseau de surveillance satellitaire communément connu sous le nom d'Echelon[130]. Dans ce cas, le Parlement européen a rappelé le souci de voir les Etats tiers y compris les

128. Comme le note Nowak (La conditionnalité relative aux droits de l'Homme, in « L'Union européenne et les droits de l'Homme », op.cit., p. 717 et la nombreuse littérature y citée): « L'importance des droits de l'Homme pour les politiques extérieures de l'UE dépasse certainement largement la PESC. A côté de l'article 130 U du traité CE (qui est maintenant son article 177), qui prévoit que la politique communautaire dans le domaine de la coopération au développement doit contribuer à la réalisation de l'objectif général de respect des droits de l'Homme et des libertés fondamentales, la CE a élaboré dans le cadre du « premier pilier » une politique extérieure dans le domaine des droits de l'Homme en préconisant notamment l'insertion de clauses spécifiques relatives à ces droits dans tous les accords conclus avec les pays tiers, en infligeant des sanctions économiques, en liant les droits de l'Homme à des préférences commerciales unilatérales, et en exécutant de vastes programmes d'assistance technique aux activités constructives dans le domaine de la démocratie et des droits de l'Homme ».

129. En ce sens, parmi d'autres auteurs, Th. Flory-N. Ligneul, art. cité, p. 182 et s.; L. Rossi, « Constitutionnalisation » de l'Union européenne et des droits fondamentaux, RTD eur., 2002; B. Brandtner-A.Rosas, Préférences commerciales et droits de l'homme, in L'Union européenne et les droits de l'homme, Ph. Alston (éd.), Bruylant, 2002, p. 729 et s.

130. Sur ce réseau et les problèmes soulevés par son existence, le lecteur se référera aux nombreux articles déjà cités consacrés à ce sujet par Yernault.

Etats-Unis d' adopter des pratiques plus respectueuses des droits de l'Homme et de souscrire à des conventions internationales en la matière[131].

Conclusions

41. La globalisation des marchés de biens et services auquel contribue de manière importante le développement des technologies de l'information et de la communication ne peut remettre en cause les acquis procurés par les législations européennes en matière de protection des données. Elle invite cependant les autorités européennes à approfondir les justifications des dispositions existantes en matière de flux transfrontières.

Ainsi, il ne suffit pas de manière négative d'affirmer que les exigences de la vie privée constituent une exception légitime aux règles du libre marché, comme le reconnaît le traité de l'Organisation mondiale du commerce et que les dispositions de la directive en matière de flux transfrontières respectent les exigences de ce traité dans la mesure où notamment le libre choix des moyens de rencontrer les exigences européennes est effectivement assuré et surtout dans la mesure où la notion de protection adéquate permet de reconnaître, loin de tout impérialisme européen, l'effectivité d'une protection fondée sur des systèmes juridiques à l'approche différente.

Il s'agit de façon beaucoup plus positive de proclamer que l'approche européenne est fondée sur une conception radicalement différente de celle qui peut prévaloir dans des pays tiers. La protection des données se fonde en dernière analyse non sur la protection d'intérêts économiques mais bien sur une conception de la dignité humaine qui exige la possibilité pour chaque personne de pouvoir s'autodéterminer dans une société de l'information où la maîtrise par chacun de sa propre image informationnelle est, chaque jour, rendue plus difficile par l'opacité des réseaux et la puissance de plus en plus grande de ceux qui traitent l'information.

42. L'objectif des législations européennes en matière de vie privée n'est pas la seule prévention ou réparation de dommages causés par des abus en matière d'utilisation de données nominatives. Au-delà, ces législations visent à créer les conditions, premièrement, pour que soit systématiquement opérée par les responsables de traitement une prise en compte des risques liberticides ou de discrimination des personnes concernées et, secondement, pour que grâce aux mécanismes de transparence, un débat à propos de ces risques puisse naître, en un premier temps, entre les personnes concernées et les responsables de traitement et, dans un second temps, de manière plus large au niveau de la société toute entière.

Si la protection des données est dans ce contexte la condition des autres libertés (celle d'obtenir du crédit, celle de se déplacer, celle de s'exprimer,...), elle exige une régulation des pouvoirs de ceux qui, tant publics que privés, traitent cette information nominative relative à autrui. L'intervention de l'Etat y trouve sa justification. Son intervention vise en effet à garantir le développement durable d'une société d'épanouissement de chacun, ce qui par ailleurs implique qu'elle limite sa propre utilisation des ressources informationnelles.

Ce devoir fondamental de l'Etat de garantir les libertés ne s'arrête pas aux limites de son propre territoire au moment où le cyberespace ne connaît plus de frontières. Il implique que le respect du droit à la vie privée reconnu comme fondamental soit garanti même lorsque l'information quitte le territoire. Ce devoir justifie les dispositions relatives aux flux

[131] Ainsi, on lit dans la résolution du parlement européen en date du 5 septembre 2001:
« Vu le traité sur l'Union européenne, en particulier l'article 6 paragraphe 2 de celui-ci qui prévoit l'obligation de respecter les droits fondamentaux...

Vu la Charte des droits fondamentaux de l'UE dont l'article 7 garantit le respect de la vie privée et familiale et prévoit le droit au respect des communications et l'article 8 protège les données à caractère personnel.

...

Considérant les déclarations faites par le Conseil..., selon lesquelles: « le Conseil ne peut accepter la création ou l'existence d'un système d'interception des télécommunications qui ne respecte pas les règles de droit des Etats membres et qui viole les principes fondamentaux visant à préserver la dignité humaine. ».

Considérant que les Etats membres ne peuvent se soustraire aux obligations qui leur incombent au titre de la Convention relative aux droits de l'Homme en faisant intervenir sur leur territoire les services de renseignements d'autre pays soumis à des dispositions moins rigoureuses car cela reviendrait à priver de ses effets le principe de légalité et ses deux composantes – accès au droit et prévisibilité de ses effets – et viderait de sa substance la jurisprudence de la Cour des droits de l'Homme.

estime nécessaire la négociation et la signature d'une convention entre l'Union européenne et les Etats-Unis établissant que chacune des deux parties respecte à l'égard de l'autre les dispositions de protection de la vie privée des citoyens et de confidentialité des communications des entreprises applicables à ses propres citoyens et entreprises.... » (Cf. également le Working Paper de l'European Parliament temporary Committee on the Echelon Interception System du 4 mai 2001 disponible sur le site http://fas.org/irp/program/process/europarl.draft.pdf)

transfrontières contenues dans les articles 25 et 26 de la directive, voire dans des cas exceptionnels, l'application extraterritoriale des lois européennes dans la mesure où la question concerne des matières d'ordre public. Au-delà, il conduit les Etats européens à une attitude plus revendicative en faveur d'une reconnaissance universelle de ce « droit » à la vie privée dans les conventions et traités internationaux.

43. Sans doute, cette attitude ne peut conduire à imposer le modèle réglementaire européen aux pays tiers. Une telle exigence irait à l'encontre des principes de l' Organisation mondiale du Commerce et au-delà de la liberté de circulation des idées, des biens et des services. Au contraire, sans exclure un devoir de vigilance[132] quant à l'effectivité d'autres approches visant à garantir de manière adéquate la protection des données, nous plaidons pour un devoir de compréhension et de respect de celles-ci. Ceci dit, l'Europe ne pourra garantir efficacement la protection de ces données, si elle ne cherche des alliés dans la technologie[133] et le « design » de l'infrastructure. La protection de la dignité humaine exige que le politique pénètre les cercles peu transparents où se décident l'architecture et les potentialités du réseau global[134].

---

132. A cet égard, on se félicite de la mise en place par la Commission de mécanismes d' évaluation des systèmes offrant des protections déclarées adéquates. Cf. à cet égard, l'évaluation réalisée par le « Commission Staff Working Paper » en application de la décision de la Commission 520/2000/CE du 26 juillet 2000 à propos des «Safe Harbor Principles» (Bruxelles 13 fév. 2002) et le commentaire critique à cet égard de J. Reidenberg, «European Commission avoids Privacy Disputes with the USA, Privacy Laws & Business Int. Newsletter, Feb. 2002, p. 9.

133. On notera que la décision du Parlement européen à propos du système Echelon insiste sur la nécessité pour l'Europe de disposer d'une politique propre en matière de cryptographie de manière à éviter les interceptions de communications électroniques par des pays tiers et que la récente directive du Parlement européen et du Conseil relative à la protection des données personnelles et de la vie privée dans le secteur des communications électroniques autorise l'établissement de normes techniques au cas où la protection des données serait mise en danger par la configuration ou le fonctionnement des terminaux (p.ex. par l'envoi automatique de données à partir de l'équipement de l'internaute).

134. Sur ces organes de régulation technique et leur importance fondamentale dans les décisions relatives à l'architecture du réseau et à son mode de fonctionnement, lire J. Berleur et Y. Poullet, « Les modes de régulation d'Internet », in L'autorégulation, Berleur, Lazaro, Queck (ed.), Cahier du Crid n° 22, Bruylant, Bruxelles, 2002, p. 133 et ss.. A cet égard, les réflexions dès 1993 de J. Reidenberg, Rules of the Road on Global Electronic Highways: Merging the Trade and Technical Paradigms, 6 Harvard Journal Law & Tech., 287 (1993) qui mettait en évidence le divorce entre l'approche législative et celle des organes techniques de régulation.